Commun. Korean Math. Soc. **20** (2005), No. 3, pp. 467–485

CONGRUENCE EQUATIONS OF $ax^i + by^j \equiv c$ AND $ax^i + by^j + dz^t \equiv c \pmod{p}$ WHEN $p = 2q + 1$ WITH p AND q ODD PRIMES

DAEYEOUL KIM*, JA KYUNG KOO**, AND MYUNG-HWAN KIM***

ABSTRACT. Let p and q be odd primes with $p = 2q + 1$. We study the number of solutions of congruence equations $ax^i + by^j \equiv c \pmod{p}$ and $ax^i + by^j + dz^t \equiv c \pmod{p}$

1. Introduction

The inspiration of this article is based on the famous paper of Weil[17]. The relationship between Gauss sums (also known as Lagrange resolvents) and Jacobi sums was examined by Gauss (unpublished), Jacobi[7], Eisenstein[5], Cauchy and others. Berndt and Evans studied Gauss, Jacobi, and other classical character sums attached to characters of order $6, 8, 12, 24$ ([2, 3]).

On the other hand, Dickson[4] computed the number of solutions of the congruence equation $x^e + y^e + 1 \equiv 0 \pmod{p = ef + 1}$ and Rajwade found the number of solutions of the congruences $y^2 - x^3 \equiv -a \pmod{p}$, $y^2 - x^3 \equiv -Dx \pmod{p}$, $y^2 - x^4 \equiv -a \pmod{p}$, $y^2 - x^5 \equiv -a \pmod{p}$, $y^2 - x^6 \equiv -a \pmod{p}$ ([10, 11, 12, 16]). Meanwhile, Sun([14, 15]) found the number of cubic and quartic residues and considered various conditions for cubic residues, nonresidues and primes. Let t be a rational prime such that $t \equiv 1 \pmod{7}$. Williams showed that a certain triple of a Diophantine system of quadratic forms has exactly six nontrivial

Received December 12, 2004.

2000 Mathematics Subject Classification: 11A07, 11D45.

Key words and phrases: congruences, counting solutions of Diophantine equations.

* This work was supported by grant No. (R08-2003-10439-0) from the Basic Research Program of the Korea Science & Engineering Foundation.

** The second author was supported by Korea Research Foundation Grant (KRF-2002-070-C00003).

*** The third author was supported by KRF Grant (KRF-2003-070-C00001).

solutions ([18, 19]). Akazawa[1] considered the case $y^2 \equiv x(x^2+2x+2) \pmod{p}$.

Let $a_1x^{l_1} + \cdots + a_rx^{l_r} \equiv b \pmod{p}$, where $a_1, \cdots, a_r \in \mathbb{Z} - \{0\}$ and $b \in \mathbb{Z}$. If $b \neq 0$ and N is the number of solutions of the above equation, then

$$N = p^{r-1} + \sum \chi_1 \cdots \chi_r(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1}) \cdots \chi_r(a_r^{-1})J(\chi_1, \cdots, \chi_r),$$

where the summation is over all r-tuples of characters $\chi_1, \cdots, \chi_r$ such that $\chi_i^{l_i} = \epsilon$ and $\chi_i \neq \epsilon$ for each $i = 1, \cdots, r$(ϵ is the trivial character). If M_0 is the number of such r-tuples with $\chi_1 \cdots \chi_r = \epsilon$, and M_1 is the number of such r-tuples with $\chi_1 \cdots \chi_r \neq \epsilon$, then

$$|N - p^{r-1}| \leq M_0 p^{(r/2)-1} + M_1 p^{(r-1)/2}.$$

For the details we refer to Ireland and Rosen's book([6, Theorem 5). In the book, they remarked :

"If p is sufficiently large, the congruence has many solutions. In fact, the number of solutions tends to infinity as p is taken larger and larger."

In Section 3, we classify the congruence equations $ax^i + by^j \equiv c \pmod{p}$, where $a, b, c, i, j \neq 0$. We are considering $(p-1)^5$ curves over $\mathbb{F}_p$.

Let p be an odd prime such that $p = 2q + 1$, where q is also an other odd prime. Throughout sections 3 and 4, we consider the number of solutions of the congruence equations by utilizing some paths which satisfy congruence equations. To this end, we need of the following notations.

Let $(a_1, l_1, a_2, l_2, \cdots, a_n, l_n, c)_p$ stand for the congruence equation

$$a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n} \equiv c \pmod{p},$$

and we write the number of solutions modulo p of $(a_1, l_1, \cdots, a_n, l_n, c)_p$ by $N(a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n} \equiv c \pmod{p})$ or simplify $|a_1, l_1, \cdots, a_n, l_n, c|_p$. We say that $(a, i, b, j, c)_p$ is *quasi-isogenous* to $(a', i', b', j', c')_p$ modulo p if $(a, i, b, j, c)_p$ and $(a', i', b', j', c')_p$ have the same number of solutions, and write $(a, i, b, j, c)_p \sim (a', i', b', j', c')_p$. The set

$$\{(a', i', b', j', c')_p | (a, i, b, j, c)_p \sim (a', i', b', j', c')_p\}$$

is called a *quasi-isogeny class modulo p*, and we denoted by $[(a, i, b, j, c)]_p$. We often omit the subscript p when no confusion may arise. We derive in

Theorem 3.19 that the number of quasi-isogeny classes of $[(a,i,b,j,c)]_p$ is 15 except when $p = 7$. More precisely, the numbers of solutions of (a,i,b,j,c) are 0, 2, $\frac{p-1}{2}$, $p-1$, p, $p+1$, $2p-2$, $2p$, $(\frac{p-1}{2})^2$, $(\frac{p^2-1}{4})$, $(p-1)^2$, $\frac{3p-3}{2}$, $\frac{p^2-p}{2}$, $\frac{(p-1)^2}{2}$ and η, where

$$\eta = \begin{cases} \frac{p+3}{2} & \text{if } q \equiv 1 \pmod 4, \\ \frac{3p+1}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

These are all distinct if $p \neq 7$. If $p = 7$, only 13 numbers 0, 2, 3, 6, 7, 8, 9, 11, 12, 14, 18, 21, 36 can be the numbers of solutions of (a,i,b,j,c).

In section 4, we find that the possible maximum number of quasi-isogeny classes $[(a,i,b,j,d,k,c)]_p$ is the following (Theorem 4.1):

$$|[(a,i,b,j,d,k,c)]_p| = \begin{cases} 139 & \text{if } q \equiv 5 \pmod{12} \text{ except } p = 11, \\ 135 & \text{if } q \equiv 11 \pmod{12} \text{ except } p = 23. \end{cases}$$

And, for instance, we determine the exact number of quasi-isogeny classes for $p = 5, 7, 11, 23$ as follows:

$$|[(a,i,b,j,d,k,c)]_p| = \begin{cases} 56 & \text{if } p = 5, \\ 68 & \text{if } p = 7, \\ 98 & \text{if } p = 11, \\ 128 & \text{if } p = 23. \end{cases}$$

We rely on Mathematica 4.0 for heavy computations.

2. Preliminaries

In this section, we define some notations and introduce some basic facts without proofs which will be used in the sequel. There are many standard books, for example [6] and [8], in which the readers can find proofs. Let (a,b) denote the *greatest common divisor* of a and b.

PROPOSITION 2.1.

(a) *If* $d|p-1$, *then* $x^d \equiv 1 \pmod p$ *has exactly* d *solutions.*
(b) *Let* $(a,m) = 1$. *If* $x^n \equiv a \pmod m$ *is solvable, then there are exactly* $(n, \phi(m))$ *solutions, where* ϕ *is the Euler* ϕ*-function.*

LEMMA 2.2. *Let* $(p-1,m)=m'$. *The congruence* $x^m \equiv x_0 \pmod p$ *is solvable if and only if* $x^{m'} \equiv x_0 \pmod p$ *is solvable.*

PROOF. If $x^m \equiv x_0 \pmod p$ is solvable, then there exist $a,t \in \mathbb{Z}$ such that $a^m = a^{m't} \equiv x_0 \pmod p$. If $x^{m'} \equiv x_0 \pmod p$, then there exist $b,s,u \in \mathbb{Z}$ such that $b^{m'} = b^{s(p-1)}b^{mu} = (b^u)^m \equiv x_0 \pmod p$. This completes the proof. □

PROPOSITION 2.3. *The congruence equation* $a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_nx_n^{l_n} \equiv c \pmod p$ *has the same number of solutions as* $a_1x_1^{l_1'} + a_2x_2^{l_2'} + \cdots + a_nx_n^{l_n'} \equiv c \pmod p$, *where* $l_1' = (l_1, p-1)$, $l_2' = (l_2, p-1)$, $\cdots$, $l_n' = (l_n, p-1)$.

PROOF. This is clear from Proposition 2.1 and Lemma 2.2. □

The number of solutions to $x^2 \equiv a \pmod p$ is given by $1+(\frac{a}{p})$, where $(\frac{a}{p})$ the Legendre symbol.

LEMMA 2.4.

(a) $\sum_{a=1}^{p-1}(\frac{a}{p}) = 0$.

(b) $\sum_{x=0}^{p-1}(\frac{ax+b}{p}) = 0$ *if* $p \nmid a$.

Through the article we adopt the following notations:

- $1 \le a,b,c,d,i,j,t \le p-1$;
- $1 \le r,r',r'' \le p-1$ with $(r,2q) = (r',2q) = (r'',2q) = 1$;
- $1 \le k,k',k'' \le q-1$;
- b^* the arithmetic inverse of b modulo p, i.e., $bb^* \equiv 1 \pmod p$;
- $|(x,0)|$ the number of solutions of $ax^i + b \cdot 0 \equiv c \pmod p$;
- $ax^i + by^j = c$ and $ax^i + by^j + dz^k = c$ stand for $ax^i + by^j \equiv c \pmod p$ and $ax^i + by^j + dz^k \equiv c \pmod p$, respectively.

3. $ax^i + by^j = c$

We consider 16 $\{i,j\}$' s

$\{1,1\}$, $\{1,2\}$, $\{1,q\}$, $\{1,2q\}$, $\{2,1\}$, $\{2,2\}$, $\{2,q\}$, $\{2,2q\}$,

$\{q,1\}$, $\{q,2\}$, $\{q,q\}$, $\{q,2q\}$, $\{2q,1\}$, $\{2q,2\}$, $\{2q,q\}$, $\{2q,2q\}$.

We classify (a,i,b,j,c) up to quasi-isogeny with the aid of Proposition 2.3.

LEMMA 3.1. $|a, 1, b, 1, c| = p$.

PROOF. Trivial. □

COROLLARY 3.2. $|a, r, b, r', c| = p$.

PROOF. It is obvious by Proposition 2.3 and Lemma 3.1. □

LEMMA 3.3. $|a, 1, b, 2, c| = p$.

PROOF. Applying b^* to the congruence $ax + by^2 = c$, we have $y^2 = b^*c - b^*ax$ when $p \nmid b^*a$. Thus the number of solutions of $y^2 = b^*c - b^*ax$ is

$$\sum_{x=0}^{p-1}(1 + (\frac{b^*c - b^*ax}{p})) = p + \sum_{x=0}^{p-1}(\frac{b^*c - b^*ax}{p}) = p$$

by Lemma 2.4. □

COROLLARY 3.4. $|a, r, b, 2k, c| = |a, 2k, b, r, c| = p$.

REMARK. As is well-known[13], $|1, 3, -1, 2, c| = p$ with $p \equiv 2 \pmod 3$. We only consider $p = 2q + 1$. Let $E_1 : y^2 = x^3 + \alpha x \pmod p$ and $E_2 : y^2 = x^3 + \beta \pmod p$ be two elliptic curves. If we ignore the point at infinity, then $|E_1| = |E_2| = p$.

In general, if we let $F_1 : y^2 = a_0x^n + \cdots + a_n$ $(a_i \in \mathbb{F}_p)$ with $p \equiv 3 \pmod 4$ and $a_0x^n + \cdots + a_n$ an odd function. Then $|F_1| = p$.

LEMMA 3.5. $|a, 1, b, q, c| = p$.

PROOF. We know that $y^q = 0, \pm 1$. If $y^q = 0$, then $ax = c$ has a solution $(a^*c, 0)$. If $y^q = \pm 1$ then $ax \pm b = c$ has q solutions each with double signs of same order. Therefore the number of solutions is p. □

COROLLARY 3.6. $|a, r, b, q, c| = |a, q, b, r, c| = p$.

LEMMA 3.7.

$$|a, 2, b, 2, c| = \begin{cases} p + 1 & \text{if } (\frac{ab}{p}) = 1, \\ p - 1 & \text{if } (\frac{ab}{p}) = -1. \end{cases}$$

PROOF. Let $(\frac{a}{p}) = (\frac{b}{p}) = 1$. Since both a and b are quadratic residues modulo p, we have $ax^2 = x'^2$ and $by^2 = y'^2$. Consider

$$\begin{aligned}
N(x'^2 + y'^2 = c) &= \sum_{u+v=c} N(x'^2 = u)N(y'^2 = v) \\
&= \sum_{u+v=c} \{1 + (\frac{u}{p})\}\{1 + (\frac{v}{p})\} \\
&= p + \sum_{u+v=c} (\frac{u}{p})(\frac{v}{p}) \\
&= p + \sum_{v=0}^{p-1} (\frac{c-v}{p})(\frac{v}{p}) \\
&= p + (\frac{c}{p})(\frac{0}{p}) + (\frac{0}{p})(\frac{c}{p}) + \sum_{v=1, v\neq c}^{p-1} (\frac{c-v}{p})(\frac{v}{p})(\frac{v^{*2}}{p}) \\
&= p + \sum_{v=1, v\neq c}^{p-1} (\frac{cv^* - 1}{p}) \\
&= p + \sum_{t=0}^{p-1} (\frac{t}{p}) - (\frac{-1}{p}) \\
&= p + 1,
\end{aligned}$$

where $t = cv^* - 1$ and $u, v \in \mathbb{F}_p$. A similar argument can be carried over when $(\frac{ab}{p}) = -1$ or $(\frac{a}{p}) = (\frac{b}{p}) = -1$. □

COROLLARY 3.8. $|a, 2k, b, 2k', c| = |a, 2, b, 2, c|$.

LEMMA 3.9. *The number of solutions of* $ax^2 + by^q = c$ *is as follows:*

(1) $|a, 2, c, q, c| = |a, 2, -c, q, c|$

$$= \begin{cases} \frac{p+3}{2} & \text{if } q \equiv 1 \pmod 4 \text{ and } (\frac{ac}{p}) = 1, \\ \frac{3p+1}{2} & \text{if } q \equiv 3 \pmod 4 \text{ and } (\frac{ac}{p}) = 1, \\ \frac{3p-3}{2} & \text{if } q \equiv 1 \pmod 4 \text{ and } (\frac{ac}{p}) = -1, \\ \frac{p-1}{2} & \text{if } q \equiv 3 \pmod 4 \text{ and } (\frac{ac}{p}) = -1. \end{cases}$$

(2) *If* $b \neq \pm c$, *then we get the following table.*

$\left(\frac{ac}{p}\right)$	$\left(\frac{a(c-b)}{p}\right)$	$\left(\frac{a(c+b)}{p}\right)$	$\lvert a, 2, b, q, c\rvert$
$+1$	$+1$	$+1$	$2p$
$+1$	$+1$	-1	$p+1$
$+1$	-1	$+1$	$p+1$
$+1$	-1	-1	2
-1	$+1$	$+1$	$2p-2$
-1	$+1$	-1	$p-1$
-1	-1	$+1$	$p-1$
-1	-1	-1	0

PROOF. If $y^q = 0$, i.e., $ax^2 = c$, then

$$|(x,0)| = \begin{cases} 2 & \text{if } (\frac{ac}{p}) = 1, \\ 0 & \text{if } (\frac{ac}{p}) = -1. \end{cases} \tag{3.9.1}$$

If $y^q = 1$, i.e., $ax^2 = c - b$, then

$$|(x,y)| = \begin{cases} q & \text{if } c = b, \\ 2q & \text{if } (\frac{a(c-b)}{p}) = 1, \\ 0 & \text{if } (\frac{a(c-b)}{p}) = -1. \end{cases} \tag{3.9.2}$$

If $y^q = -1$, i.e., $ax^2 = c + b$, then

$$|(x,y)| = \begin{cases} q & \text{if } c = -b, \\ 2q & \text{if } (\frac{a(c+b)}{p}) = 1, \\ 0 & \text{if } (\frac{a(c+b)}{p}) = -1. \end{cases} \tag{3.9.3}$$

Let $(\frac{ac}{p}) = 1$, $b = c$, $b = -c$. Then It is impossible.

Let $(\frac{ac}{p}) = 1$, $b = c$, $(\frac{a(b+c)}{p}) = 1$. Then $1 = (\frac{a(b+c)}{p}) = (\frac{2ac}{p}) = (\frac{2}{p})$ if and only if $q \equiv 3 \pmod 4$.

By (3.9.1)$\sim$(3.9.3), we deduce that

$$|a, 2, c, q, c| = 2 + q + 2q = \frac{3p+1}{2},$$

where $(\frac{ac}{p}) = 1$ and $q \equiv 3 \pmod 4$.

Other cases can be shown in a similar manner. □

COROLLARY 3.10. $|a, 2k, b, q, c| = |a, q, b, 2k, c| = |a, 2, b, q, c|$.

LEMMA 3.11.

(1) $|a, q, a, q, a| = |-a, q, a, q, a| = |a, q, -a, q, a| = |a, q, a, q, -a| = p - 1$.

(2) $|2a, q, a, q, a| = |-2a, q, a, q, a| = |2a, q, -a, q, a| = |2a, q, a, q, -a| = |a, q, 2a, q, a| = |a, q, -2a, q, a| = |a, q, -2a, q, -a| = |a, q, 2a, q, -a| = \frac{p^2-1}{4}$.

(3) *If* $\alpha \neq \pm a, \pm 2a$, *then* $|\alpha, q, a, q, a| = |\alpha, q, -a, q, a| = |a, q, \alpha, q, a| = |a, q, \alpha, q, -a| = \frac{p-1}{2}$.

(4) *If*

$$\begin{cases} a + b = c \text{ and } c \neq -a, -b & \text{or} \\ a - b = c \text{ and } c \neq -a, b & \text{or} \\ -a + b = c \text{ and } c \neq a, -b & \text{or} \\ -a - b = c \text{ and } c \neq a, b, \end{cases}$$

then $|a, q, b, q, c| = (\frac{p-1}{2})^2$.

(5) *Otherwise,* $|a, q, b, q, c| = 0$.

PROOF. Put $x^q = 0, 1$ or -1 and $y^q = 0, 1$ or -1.
If $x^q = 0$ and $y^q = 0$, then $0 = c$.
If $x^q = 0$ and $y^q = 1$, then $b = c$.
If $x^q = 0$ and $y^q = -1$, then $-b = c$.
If $x^q = 1$ and $y^q = 0$, then $a = c$.
If $x^q = 1$ and $y^q = 1$, then $a + b = c$.
If $x^q = 1$ and $y^q = -1$, then $a - b = c$.
If $x^q = -1$ and $y^q = 0$, then $-a = c$.
If $x^q = -1$ and $y^q = 1$, then $-a + b = c$.
If $x^q = -1$ and $y^q = -1$, then $-a - b = c$.
By the assumption we know that $c \neq 0$.

Case 1. $b = c$

If $-b = c, a + b = c, -a + b = c$, then $abc = 0$, which is impossible by the hypothesis.

If $a = c$, then $|a, q, a, q, a| = p - 1$.
If $a - b = c$, then $|2a, q, a, q, a| = \frac{p^2-1}{4}$.
If $-a = c$, then $|-a, q, a, q, a| = p - 1$.
If $-a - b = c$, then $|-2a, q, a, q, a| = \frac{p^2-1}{4}$.
If $\alpha \neq \pm a, \pm 2a$, then $|\alpha, q, a, q, a| = \frac{p-1}{2}$.
Other cases can be shown in a similar way. □

REMARK. A rather general result can be found in [4, p.398].

LEMMA 3.12. $|a, 2q, b, 1, c| = p$.

PROOF. Put $x^{2q} = 0$ or 1.
If $x^{2q} = 0$, then $by = c$ and hence $|(0, y)| = 1$.
If $x^{2q} = 1$, then $by = c - a$ and hence $|(x, y)| = 2q$. Therefore there are exactly p solutions. □

COROLLARY 3.13. $|a, 2q, b, r, c| = |a, r, b, 2q, c| = |a, 2q, b, 1, c| = p$.

LEMMA 3.14.

$$|a, 2, b, 2q, c| = \begin{cases} 0 & \text{if } (\frac{ac}{p}) = (\frac{a(c-b)}{p}) = -1 \\ 2 & \text{if } (\frac{ac}{p}) = 1, (\frac{a(c-b)}{p}) = -1 \\ p-1 & \text{if } (\frac{ac}{p}) = -1, b = c \\ p+1 & \text{if } (\frac{ac}{p}) = 1, b = c \\ 2p-2 & \text{if } (\frac{ac}{p}) = -1, (\frac{a(c-b)}{p}) = 1 \\ 2p & \text{if } (\frac{ac}{p}) = (\frac{a(c-b)}{p}) = 1. \end{cases}$$

PROOF. Let $y^{2q} = 0$ or 1.
If $y^{2q} = 0$ and $(\frac{ac}{p}) = 1$(resp., -1), then $|(x, 0)| = 2$(resp., 0).
If $y^{2q} = 1$ and $b = c$, then $|(x, y)| = 2q$.
If $y^{2q} = 1$ and $b \neq c$, then

$$|(x, y)| = \begin{cases} 0 & \text{if } (\frac{a(c-b)}{p}) = -1, \\ 4q & \text{if } (\frac{a(c-b)}{p}) = 1. \end{cases}$$

From these follows the lemma. □

COROLLARY 3.15. $|a, 2q, b, 2k, c| = |a, 2q, b, 2k, c| = |a, 2, b, 2q, c|$.

The following two lemmas can be proved in a very similar manner to Lemma 3.14.

LEMMA 3.16.

(1) $|a, q, a, 2q, a| = |-a, q, a, 2q, a| = \frac{3(p-1)}{2}$.
(2) *If* $\alpha \neq \pm a$, *then* $|\alpha, q, a, 2q, a| = p - 1$.
(3) *If* $b \neq c, a + b \neq c$, *then* $|a, q, b, 2q, -a| = \frac{p-1}{2}$.

If $\alpha \neq a, 2a$, *then* $|a, q, \alpha, 2q, a| = \frac{p-1}{2}$.

(4) $|a, q, 2a, 2q, a| = |a, q, -2a, 2q, -a| = \frac{p^2-p}{2}$.

(5) *Let* $a + b = c$. *If* $-a \neq c$, *then* $|a, q, b, 2q, c| = \frac{(p-1)^2}{2}$.

Let $-a + b = c$. *If* $a \neq c$, *then* $|a, q, b, 2q, c| = \frac{(p-1)^2}{2}$.

(6) $|a, q, b, 2q, c| = 0$, *otherwise.*

COROLLARY 3.17. $|a, q, b, 2q, c| = |a, 2q, b, q, c|$.

LEMMA 3.18.

(1) $|a, 2q, a, 2q, a| = 2(p-1)$.

(2) *If* $\alpha \neq a$, *then* $|\alpha, 2q, a, 2q, a| = |a, 2q, \alpha, 2q, a| = p - 1$.

(3) *If* $a + b = c$, *then* $|a, 2q, b, 2q, c| = (p-1)^2$.

(4) $|a, 2q, b, 2q, c| = 0$, *otherwise.*

Observe that 0, 2, $\frac{p-1}{2}$, $p-1$, p, $p+1$, $2p-2$, $2p$, $(\frac{p-1}{2})^2$, $(\frac{p^2-1}{4})$, $(p-1)^2$, $\frac{3p-3}{2}$, $\frac{p+3}{2}$, $\frac{3p+1}{2}$, $\frac{p^2-p}{2}$, $\frac{(p-1)^2}{2}$ are all distinct except when $p = 7$. If $p = 7$, then $2p-2 = \frac{p^2-1}{4}$, $\left(\frac{p-1}{2}\right)^2 = \frac{3p-3}{2}$ and the others are distinct.

From Lemma 3.1$\sim$ 3.18 and the above observation, we deduce the following theorem.

THEOREM 3.19. *The number of distinct quasi-isogeny classes of* $[a, i, b, j, c]_p$ *is* 15 *except when* $p = 7$, *i.e., the values of* $|a, i, b, j, c|$ *are*

$$0,\ 2,\ \frac{p-1}{2},\ p-1,\ p,\ p+1,\ 2p-2,\ 2p,\ (\frac{p-1}{2})^2,$$
$$(\frac{p^2-1}{4}),\ (p-1)^2,\ \frac{3p-3}{2},\ \frac{p^2-p}{2},\ \frac{(p-1)^2}{2},\ \eta,$$

where

$$\eta = \begin{cases} \frac{p+3}{2} & \text{if } q \equiv 1 \pmod 4, \\ \frac{3p+1}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

When $p = 7$, *the number of quasi-isogeny classes of* $[a, i, b, j, c]_7$ *is* 13, *i.e., the values of* $|a, i, b, j, c|$ *are* 0, 2, 3,6, 7, 8, 9,11, 12, 14,18,21 *and* 36.

More precisely ; let a, b *and* c *be distinct numbers in* $\mathbb{F}_p^*$.

(1) *If* $q \equiv 1 \pmod 4$, *then the quasi-isogeny classes are the following:*

Case 1. $|a, i, b, j, c| = p$.

(a,i,b,j,c)	*condition*
(a,r,b,r',c) $(a,r,b,2k,c),(b,2k,a,r,c)$ $(a,r,b,q,c),(b,q,a,r,c)$ $(a,2q,b,r,c),(b,r,a,2q,c)$	$\times$

Case 2. $|a,i,b,j,c| = p+1$

(a,i,b,j,c)	condition
$(a,2k,b,2k',c)$	$(\frac{ab}{p}) = 1$
$(a,2k,b,q,c),(b,q,a,2k,c)$	$(\frac{ac}{p}) = 1, (\frac{a(c-b)}{p}) = -(\frac{a(c+b)}{p}) \neq 0$
$(a,2k,b,2q,b),(b,2q,a,2k,b)$	$(\frac{ab}{p}) = 1$

Case 3. $|a,i,b,j,c| = p-1$

(a,i,b,j,c)	*condition*
$(a,2k,b,2k',c)$	$(\frac{ab}{p}) = -1$
$(a,2k,a,q,c),(a,q,a,2k,c)$	$(\frac{ac}{p}) = -1, (\frac{a(c+a)}{p}) = -(\frac{a(c-a)}{p}) \neq 0$
$(a,2k,b,q,c),(b,q,a,2k,c)$	$(\frac{ac}{p}) = -1, (\frac{a(c-b)}{p}) = -(\frac{a(c+b)}{p}) \neq 0$
$(\alpha,q,a,2q,a),(a,2q,\alpha,q,a)$	$\alpha \neq \pm a$
$(\alpha,2q,a,2q,a),(a,2q,\alpha,2q,a)$	$\alpha \neq a$
$(a,q,a,q,a),(a,q,a,q,-a)$ $(-a,q,a,q,a),(a,q,-a,q,a)$	$\times$

Case 4. $|a,i,b,j,c| = 2p$

(a,i,b,j,c)	*condition*
$(a,2k,b,2q,c),(b,2q,a,2k,c)$	$(\frac{ac}{p}) = (\frac{a(c-b)}{p}) = 1$

Case 5. $|a,i,b,j,c| = 2$

(a,i,b,j,c)	*condition*
$(a,2k,b,2q,c),(b,2q,a,2k,c)$	$(\frac{ac}{p}) = 1, (\frac{a(c-b)}{p}) = -1$

Case 6. $|a,i,b,j,c| = 2(p-1)$

(a,i,b,j,c)	*condition*
$(a,2k,-a,2q,c),(-a,2q,a,2k,c)$	$(\frac{ac}{p}) = -1, (\frac{a(c+a)}{p}) = 1$
$(a,2k,b,2q,c),(b,2q,a,2k,c)$	$(\frac{ac}{p}) = -1, (\frac{a(c-b)}{p}) = 1$
$(a,2q,a,2q,a)$	$\times$

Case 7. $|a,i,b,j,c| = (\frac{p-1}{2})^2$

(a,i,b,j,c)	*condition*
(a,q,b,q,c)	$a+b=c$ *and* $c \neq -a,-b$ *or* $a-b=c$ *and* $c \neq a,b$ *or* $-a+b=c$ *and* $c \neq a,-b$ *or* $-a-b=c$ *and* $c \neq a,b$

Case 8. $|a,i,b,j,c| = \frac{p^2-1}{4}$

(a,i,b,j,c)	*condition*
$(2a,q,a,q,a),(2a,q,-a,q,a)$ $(2a,q,-a,q,a),(2a,q,a,q,-a)$ $(a,q,2a,q,a),(a,q,-2a,q,a)$ $(a,q,-2a,q,-a),(a,q,2a,q,-a)$	$\times$

Case 9. $|a,i,b,j,c| = (p-1)^2$

(a,i,b,j,c)	*condition*
$(a,2q,b,2q,a+b)$	$\times$

Case 10. $|a,i,b,j,c| = \frac{p^2-p}{2}$

(a,i,b,j,c)	*condition*
$(a,q,2a,2q,a),(2a,2q,a,q,a)$ $(a,q,-2a,2q,-a),(-2a,2q,a,q,-a)$	$\times$

Case 11. $|a,i,b,j,c| = \frac{(p-1)^2}{2}$

(a,i,b,j,c)	*condition*
$(a,q,b,2q,a+b),(a,2q,b,q,a+b)$	$-a \neq c$
$(a,q,b,2q,-a+b),(a,2q,b,q,-a+b)$	$a \neq c$

Case 12. $|a,i,b,j,c| = 0$

(a,i,b,j,c)	*condition*
$(a,2k,b,q,c),(b,q,a,2k,c)$	$(\frac{ac}{p}) = (\frac{a(c-b)}{p}) = (\frac{a(c+b)}{p}) = -1$
$(a,2k,b,2q,c),(b,2q,a,2k,c)$	$(\frac{ac}{p}) = (\frac{a(c-b)}{p}) = -1$
(a,q,b,q,c)	$(*1)$
$(a,q,b,2q,c)$	$(*2)$
$(a,2q,b,2q,c)$	$(*3)$

Here, the condition $(*1)$ *for* (a,q,b,q,c) *is that* a,b *and* c *are none*

of the following:

$$\begin{cases} a = b = c \ \text{ or } a = b, c = -a \text{ or } b = c, a = -b \ \text{ or } a = c, b = -a; \\ c = \pm b, a = \pm 2b \ \text{ or } c = \pm a, b = \pm 2a; \\ a + b = c \ \text{ or } a - b = c \ \text{ or } \ -a + b = c \ \text{ or } \ -a - b = c, \\ \ \text{where } c \neq \pm a, \pm b; \\ c = \pm a, b \neq \pm 2a, \pm a \text{ or } c = \pm b, a \neq \pm 2b, \pm b. \end{cases}$$

The condition $(*2)$ *for* $(a, q, b, 2q, c)$ *is that* a, b *and* c *are none of the following:*

$$\begin{cases} a = b = c \text{ or } \ -a = b = c; \\ a \neq \pm b \ \text{ and } b = c; \\ b \neq c, a + b \neq c \ \text{ and } \ -a = c; \\ b \neq a, 2a \text{ and } a = c; \\ a = c, b = 2a \text{ or } \ -a = c, b = -2a; \\ a + b = c, -a \neq c \text{ or } \ -a + b = c, a \neq c. \end{cases}$$

The condition $(*3)$ *for* $(a, 2q, b, 2q, c)$ *is that* a, b *and* c *are none of the following:*

$$\begin{cases} c = a + b; \\ a = b = c; \\ a = c, b \neq a \text{ or } b = c, a \neq b. \end{cases}$$

Case 13. $|a, i, b, j, c| = \frac{3(p-1)}{2}$

(a, i, b, j, c)	*condition*
$(a, 2k, c, q, c), (c, q, a, 2k, c)$ $(a, 2k, -c, q, c), (-c, q, a, 2k, c)$	$(\frac{ac}{p}) = -1$
$(a, q, a, 2q, a), (a, 2q, a, q, a)$ $(-a, q, a, 2q, a), (a, 2q, -a, q, a)$	$\times$

Case 14. $|a, i, b, j, c| = \frac{p+3}{2}$

(a, i, b, j, c)	*condition*
$(a, 2k, a, q, c), (a, q, a, 2k, c)$ $(a, 2k, -c, q, c), (-c, q, a, 2k, c)$	$(\frac{ac}{p}) = -1$

Case 15. $|a, i, b, j, c| = \frac{p-1}{2}$

(a,i,b,j,c)	*condition*
$(a,q,b,2q,-a),(a,2q,b,q,-b)$	$b \neq c, a+b \neq c$
$(a,q,\alpha,2q,a),(\alpha,2q,a,q,a)$	$\alpha \neq a, 2a$
$(\alpha,q,a,q,a),(\alpha,q,-a,q,a)$ $(a,q,\alpha,q,a),(a,q,\alpha,q,-a)$	$\alpha \neq \pm a, \pm 2a$

(2) *If* $q \equiv 3 \pmod 4$, *then the quasi-isogeny classes are the following: Case 1 through Case 12 are the same are* (1).

Case 13. $|a,i,b,j,c| = \frac{3(p-1)}{2}$

(a,i,b,j,c)	*condition*
$(a,2k,c,q,c),(c,q,a,2k,c)$ $(a,2k,-c,q,c),(-c,q,a,2k,c)$	$(\frac{ac}{p}) = -1$
$(a,q,a,2q,a),(a,2q,a,q,a)$ $(-a,q,a,2q,a),(a,2q,-a,q,a)$	$\times$

Case 14. $|a,i,b,j,c| = \frac{3p+1}{2}$

(a,i,b,j,c)	*condition*
$(a,2k,c,q,c),(c,q,a,2k,c)$ $(a,2k,-c,q,c),(-c,q,a,2k,c)$	$(\frac{ac}{p}) = 1$

Case 15. $|a,i,b,j,c| = \frac{p-1}{2}$

(a,i,b,j,c)	*condition*
$(\alpha,q,-a,q,a),(\alpha,q,a,q,a)$ $(a,q,\alpha,q,a),(a,q,\alpha,q,-a)$	$\alpha \neq \pm a, \pm 2a$
$(a,q,b,2q,-a),(b,2q,a,q,-b)$	$b \neq c, a+b \neq c$
$(a,q,\alpha,2q,a),(\alpha,2q,a,q,a)$	$\alpha \neq a, 2a$

REMARK. When $p = 5$, on can easily find that $|a,i,b,j,c| = 0, 2, 4, 5, 6, 8, 10, 16$.

REMARK. In Asiacrypt 1999, Y. Tsuruoka and N. Kunihiro proposed a problem:

"Let c, x, y be integers such that $0 \leq x, y < c$. Let $N(c)$ be the number of points (x,y) satisfying $y^2 \equiv x^3 + 11x \pmod c$. Find all values of c such that $N(c) = 1999$."

We may ask more generally:

For $a,i,b,j,c \in F_p^*$, find all values of p such that $|a,i,b,j,c| = 1999$. Theorem 3.19 tells us that there is a unique prime p, which is 1999. Another approach is in [9].

4. $ax^i + by^j + dz^t = c$

In this section, we consider the number of solutions of $ax^i+by^j+dz^t = c$ by using the results of section 3. By Proposition 2.3, we may consider 64 cases of $\{i, j, t\}$'s with $i, j, k \in \{1, 2, q, 2q\}$.

In a similar way, when working with all cases, we derive the following:

THEOREM 4.1.

(1) *If $q \equiv 5 \pmod{12}$ except for $p = 11$, then the possible maximum number of quasi-isogeny classes of $[a, i, b, j, d, k, c]_p$ is 139, in other words,*
$|a, i, b, j, d, k, c| = 0,\ 2,\ \frac{p-1}{2},\ \frac{p+3}{2},\ p-1,\ p+1,\ \frac{3p-3}{2},\ 2p-2,\ 2p,\ \frac{5p-1}{2},\ 3p-3,\ 3p-1,\ \frac{7p-7}{2},\ 4p-4,\ 4p-2,\ \frac{p^2-2p+1}{4},\ \frac{p^2-1}{4},\ \frac{p^2+2p-3}{4},\ \frac{p^2+4p-5}{4},\ \frac{p^2+6p+1}{4},\ \frac{p^2+10p-3}{4},\ \frac{p^2+14p-7}{4},\ \frac{p^2-2p+1}{2},\ \frac{p^2-2p+5}{2},\ \frac{p^2-p+4}{2},\ \frac{p^2-p}{2},\ \frac{p^2-1}{2},\ \frac{p^2+3}{2},\ \frac{p^2+p-2}{2},\ \frac{p^2+p+2}{2},\ \frac{p^2+2p-3}{2},\ \frac{p^2+2p+1}{2},\ \frac{p^2+3p-4}{2},\ \frac{p^2+3p}{2},\ \frac{p^2+4p-5}{2},\ \frac{p^2+4p-1}{2},\ \frac{p^2+5p-6}{2},\ \frac{p^2+6p-7}{2},\ \frac{p^2+6p-3}{2},\ \frac{3p^2-6p+3}{4},\ \frac{3p^2-4p+1}{4},\ \frac{3p^2-2p+7}{4},\ \frac{3p^2+2p-5}{4},\ \frac{3p^2+2p+3}{4},\ \frac{3p^2+4p-7}{4},\ \frac{3p^2+6p-1}{4},\ \frac{3p^2+6p-9}{4},\ \frac{3p^2+10p-13}{4},\ \frac{2p^2-3p+1}{2},\ (p-1)^2,\ p^2-2p+3,\ \frac{2p^2-3p+5}{2},\ p^2-p,\ p^2-p+2,\ \frac{2p^2-p-1}{2},\ \frac{2p^2-p+3}{2},\ p^2-1,\ p^2,\ p^2+1,\ \frac{2p^2+p-3}{2},\ \frac{2p^2+p+1}{2},\ p^2+p-2,\ p^2+p,\ \frac{2p^2+3p-5}{2},\ p^2+2p-3,\ p^2+2p-1,\ \frac{5p^2-10p+13}{4},\ \frac{5}{4}(p-1)^2,\ \frac{5p^2-6p+9}{4},\ \frac{5p^2-6p+1}{4},\ \frac{5p^2-4p+7}{4},\ \frac{5p^2-2p-3}{4},\ \frac{5p^2-2p+5}{4},\ \frac{5p^2+2p-7}{4},\ \frac{3p^2-6p+3}{2},\ \frac{3p^2-6p+7}{2},\ \frac{3p^2-5p+2}{2},\ \frac{3p^2-5p+6}{2},\ \frac{3p^2-4p+1}{2},\ \frac{3p^2-4p+5}{2},\ \frac{3p^2-3p}{2},\ \frac{3p^2-3p+4}{2},\ \frac{3p^2-2p-1}{2},\ \frac{3p^2-2p+3}{2},\ \frac{3p^2-p-2}{2},\ \frac{3p^2-p+2}{2},\ \frac{3p^2-3}{2},\ \frac{3p^2+1}{2},\ \frac{3p^2+p-4}{2},\ \frac{3p^2+2p-5}{2},\ \frac{3p^2+2p-1}{2},\ \frac{7p^2-14p+7}{4},\ \frac{7p^2-10p+3}{4},\ \frac{7p^2-6p-1}{4},\ 2p^2-4p+2,\ 2p^2-4p+4,\ \frac{4p^2-7p+7}{2},\ 2p^2-3p+1,\ 2p^2-3p+3,\ \frac{4p^2-5p+1}{2},\ 2p^2-2p,\ 2p^2-2p+2,\ \frac{4p^2-3p+3}{2},\ 2p^2-p-1,\ 2p^2-p+1,\ \frac{4p^2-p-3}{2},\ 2p^2-2,\ 2p^2,\ 3(p-1)^2,\ \frac{p^3-3p^2+3p-1}{8},\ \frac{p^3-3p^2+7p-5}{8},\ \frac{p^3-3p^2+11p-9}{8},\ \frac{p^3-p^2-p+1}{8},\ \frac{p^3-p^2+3p-3}{8},\ \frac{p^3+p^2-5p+3}{8},\ \frac{3p^3-9p^2+21p-15}{8},\ \frac{(p-1)^3}{4},\ \frac{p^3-3p^2+5p-3}{4},\ \frac{p^3-3p^2+7p-5}{4},\ \frac{p^3-2p^2+3p-2}{4},\ \frac{p^3-2p^2+p}{4},\ \frac{p^3-p^2-p+1}{4},\ \frac{p^3-p^2+p-1}{4},\ \frac{p^3-3p+2}{4},\ \frac{p^3-p}{4},\ \frac{2p^3-5p^2+8p-5}{4},\ \frac{(p-1)^3}{2},\ \frac{p^3-3p^2+4p-2}{2},\ \frac{p^3-3p^2+5p-3}{2},\ \frac{p^3-3p^2+6p-4}{2},\ \frac{p^3-3p^2+7p-5}{2},\ \frac{p^3-3p^2+8p-6}{2},\ \frac{p^3-2p^2+p}{2},\ \frac{p^3-2p^2+2p-1}{2},\ \frac{p^3-2p^2+3p-2}{2},\ \frac{p^3-p^2-p+1}{2},\ (p-1)^3,\ p^3-3p^2+4p-2,\ p^3-3p^2+5p-3.$

(2) *And if $p = 11$, then the exact number of quasi-isogeny classes of $[a, i, b, j, d, k, c]_{11}$ is 98, in other words,*

$|a,i,b,j,d,k,c|_{11}$= *0, 2, 5, 7, 10, 12, 15, 20, 22, 25, 27, 30, 32, 35, 40, 42, 50, 55, 57, 60, 65, 70, 72, 75, 77, 80, 82, 85, 87, 90, 92, 100, 102, 105, 107, 110, 112, 115, 117, 120, 121, 122, 125, 127, 130, 132, 135, 140, 142, 150, 152, 155, 157, 160, 162, 165, 170, 172, 175, 185, 200, 202, 207, 210, 212, 215, 220, 222, 227, 230, 232, 235, 240, 242, 250, 255, 260, 275, 280, 300, 305, 325, 330, 390, 500, 505, 510, 515, 520, 525, 535, 550, 555, 560, 600, 1000, 1010, 1020.*

(3) *If* $q \equiv 11 \pmod{12}$ *except for* $p = 23$, *then the possible maximum number of quasi-isogeny classes of* $[a,i,b,j,d,k,c]_p$ *is* 135, *in other words,*

$|a,i,b,j,d,k,c| = 0,\ 2,\ \frac{p-1}{2},\ p-1,\ p+1,\ \frac{3p-3}{2},\ \frac{3p+1}{2},\ 2p-2,\ 2p,$
$\frac{5p-5}{2},\ 3p-3,\ 3p-1,\ \frac{7p-3}{2},\ 4p-4,\ 4p-2,\ \frac{p^2-2p+1}{4},\ \frac{p^2-1}{4},\ \frac{p^2+2p-3}{4},$
$\frac{p^2+4p-5}{4},\ \frac{p^2+6p-7}{4},\ \frac{p^2-2p+1}{2},\ \frac{p^2-2p+5}{2},\ \frac{p^2-p}{2},\ \frac{p^2-1}{2},\ \frac{p^2+3}{2},\ \frac{p^2+p-2}{2},$
$\frac{p^2+p+2}{2},\ \frac{p^2+2p-3}{2},\ \frac{p^2+2p+1}{2},\ \frac{p^2+3p-4}{2},\ \frac{p^2+3p}{2},\ \frac{p^2+4p-5}{2},\ \frac{p^2+4p-1}{2},$
$\frac{p^2+5p-2}{2},\ \frac{p^2+6p-7}{2},\ \frac{p^2+6p-3}{2},\ \frac{3p^2-6p+11}{4},\ \frac{3p^2-6p+3}{4},\ \frac{3p^2-4p+1}{4},$
$\frac{3p^2-2p+7}{4},\ \frac{3p^2-2p-1}{4},\ \frac{3p^2-3}{4},\ \frac{3p^2+2p-5}{4},\ \frac{3p^2+2p+3}{4},\ \frac{3p^2+6p-9}{4},$
$\frac{2p^2-3p+1}{2},\ (p-1)^2,\ p^2-2p+3,\ \frac{2p^2-3p+1}{2},\ p^2-p,\ p^2-p+2,\ \frac{2p^2-p-1}{2},$
$\frac{2p^2-p+3}{2},\ p^2-1,\ p^2,\ p^2+1,\ \frac{2p^2+p-3}{2},\ \frac{2p^2+p+1}{2},\ \frac{2p^2+3p-1}{2},\ p^2+p-2,$
$p^2+p,\ p^2+2p-3,\ p^2+2p-1,\ \frac{5}{4}(p-1)^2,\ \frac{5p^2-6p+9}{4},\ \frac{5p^2-2p-3}{4},$
$\frac{5p^2-2p+5}{4},\ \frac{5p^2+3}{4},\ \frac{5p^2+2p-7}{4},\ \frac{5p^2+2p+1}{4},\ \frac{5p^2+6p-11}{4},\ \frac{3p^2-6p+3}{2},$
$\frac{3p^2-6p+7}{2},\ \frac{3p^2-5p+2}{2},\ \frac{3p^2-4p+1}{2},\ \frac{3p^2-4p+5}{2},\ \frac{3p^2-3p}{2},\ \frac{3p^2-3p+4}{2},$
$\frac{3p^2-2p-1}{2},\ \frac{3p^2-2p+3}{2},\ \frac{3p^2-p-2}{2},\ \frac{3p^2-p+2}{2},\ \frac{3p^2-3}{2},\ \frac{3p^2+1}{2},\ \frac{3p^2+p}{2},$
$\frac{3p^2+2p-5}{2},\ \frac{3p^2+2p-1}{2},\ \frac{7p^2-6p+7}{4},\ \frac{7p^2-2p+3}{4},\ \frac{7p^2+2p-1}{4},\ 2p^2-4p+2,$
$2p^2-4p+4,\ 2p^2-3p+1,\ 2p^2-3p+3,\ \frac{4p^2-7p+3}{2},\ \frac{4p^2-5p+5}{2},\ 2p^2-2p,$
$2p^2-2p+2,\ \frac{4p^2-3p-1}{2},\ 2p^2-p-1,\ 2p^2-p+1,\ \frac{4p^2-p+1}{2},\ 2p^2,$
$3(p-1)^2,\ \frac{p^3-3p^2+3p-1}{8},\ \frac{p^3-3p^2+7p-5}{8},\ \frac{p^3-3p^2+11p-9}{8},\ \frac{p^3-p^2-p+1}{8},$
$\frac{p^3-p^2+3p-3}{8},\ \frac{p^3+p^2-5p+3}{8},\ \frac{3p^3-9p^2+21p-15}{8},\ \frac{(p-1)^3}{4},\ \frac{p^3-3p^2+5p-3}{4},$
$\frac{p^3-3p^2+7p-5}{4},\ \frac{p^3-2p^2+3p-2}{4},\ \frac{p^3-2p^2+p}{4},\ \frac{p^3-p^2-p+1}{4},\ \frac{p^3-p^2+p-1}{4},$
$\frac{p^3-3p+2}{4},\ \frac{p^3-p}{4},\ \frac{2p^3-5p^2+8p-5}{4},\ \frac{(p-1)^3}{2},\ \frac{p^3-3p^2+4p-2}{2},\ \frac{p^3-3p^2+5p-3}{2},$
$\frac{p^3-3p^2+6p-4}{2},\ \frac{p^3-3p^2+7p-5}{2},\ \frac{p^3-3p^2+8p-6}{2},\ \frac{p^3-2p^2+p}{2},\ \frac{p^3-2p^2+2p-1}{2},$
$\frac{p^3-2p^2+3p-2}{2},\ \frac{p^3-p^2-p+1}{2},\ (p-1)^3,\ p^3-3p^2+4p-2,\ p^3-3p^2+5p-3.$

(4) *And if* $p = 23$, *then the exact number of quasi-isogeny classes of* $[a,i,b,j,d,k,c]_{23}$ *is* 128, *in other words,*

$|a, i, b, j, d, k, c| = 0, 2, 11, 22, 24, 33, 35, 44, 46, 55, 66, 68, 79, 88, 90, 121, 132, 143, 154, 165, 242, 244, 253, 264, 266, 275, 277, 286, 288, 299, 308, 310, 321, 330, 332, 363, 365, 374, 387, 396, 407, 409, 429, 484, 486, 495, 506, 508, 517, 519, 528, 529, 530, 539, 541, 550, 552, 563, 572, 574, 605, 629, 649, 651, 662, 671, 693, 726, 728, 737, 748, 750, 759, 770, 772, 781, 783, 792, 794, 814, 816, 893, 915, 937, 968, 970, 979, 990, 992, 1003, 1012, 1014, 1023, 1034, 1036, 1047, 1056, 1058, 1331, 1342, 1353, 1452, 1463, 1573, 2662, 2673, 2684, 2783, 2794, 2904, 2915, 3025, 3036, 4026, 5324, 5335, 5346, 5357, 5368, 5379, 5467, 5566, 5577, 5588, 5808, 10648, 10670, 10692.$

(5) *And if $p = 7$, then the exact number of quasi-isogeny classes of $[a, i, b, j, d, k, c]_7$ is 68, in other words,*
$|a, i, b, j, d, k, c| = 0, 2, 3, 6, 8, 9, 12, 14, 15, 18, 20, 21, 23, 24, 26, 27, 29, 30, 33, 35, 36, 38, 39, 42, 44, 45, 47, 48, 49, 50, 51, 53, 54, 56, 57, 59, 60, 62, 63, 66, 68, 69, 72, 74, 75, 77, 78, 80, 81, 83, 84, 86, 90, 92, 96, 108, 111, 114, 117, 120, 123, 126, 129, 132, 144, 216, 222, 228.$

REMARK. If we can find $a, b, c, d \in \mathbb{F}_p^*$ satisfying the conditions in Theorem 4.1 (for example, $(\frac{ac}{p}) = (\frac{ab}{p}) = (\frac{a(2c-b)}{p}) = (\frac{a(c-b)}{p}) = (\frac{-a(c+b)}{p}) = 1$), then the number of quasi-isogeny classes of $|a, i, b, j, d, k, c|_p$ is 139 or 135. If p is sufficiently large, then we conjecture that the number of quasi-isogeny classes of $|a, i, b, j, d, k, c|_p$ is 139 or 135, that is, we can replace the possible maximum number by the one listed in Theorem 4.1.

REMARK. If $p = 5$, then the exact number of quasi-isogeny classes of $[a, i, b, j, d, k, c]_5$ is 56, in other words, $|a, i, b, j, d, k, c|_p = 0$, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 51, 52, 53, 54, 56, 57, 59, 70.

References

[1] H. Akazawa, *The congruence relations of the number of $\mathbb{F}_p$-rational points on $y^2 = x(x^2 + 2x + 2)$*, Math. J. Okayama Univ. **42** (2000), 67–71.

[2] B. C. Berndt, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory **11** (1979), 349–398.

[3] B. C. Berndt and R. C. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. **23** (1979), 374–437.

[4] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
[5] G. Eisenstein, *Beiträge zur Kreisteilung*, J. Reine Angew. Math. (1844), 269–278.
[6] K. Ireland and M. Rosen, *A Classical Introduction to Mordern Number Theory*, Springer-Verlag, 1981.
[7] C. Jacobi, *Über die Kreisteilung ...*, J. Reine Angew. Math. (1846), 254–274.
[8] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, John Wiley & Sons, Inc., 1991.
[9] A. Pekin and H. Icscan, *On the solvability of the equation* $x^2 - py^2 = \pm q$ *and the class number of* $\mathbb{Q}(\sqrt{p})$ *for the* $p = [(2n+1)q]^2 \pm 1$, Adv. Stud. Contemp. Math. (2004), 87–92, 254–274.
[10] A. R. Rajwade, *A note on the number of solutions* N_p *of the congruence* $y^2 \equiv x^3 - Dx \pmod{p}$, Proc. Cambridge Phil. Soc. **67** (1970), 603–605.
[11] ———, *On rational primes p congruent to 1(mod 3 or 5)*, Proc. Cambridge Phil. Soc. **66** (1969), 61–70.
[12] ———, *On the congruence* $y^2 \equiv x^5 - a \pmod{p}$, Proc. Cambridge Phil. Soc. **74** (1973), 473–475.
[13] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
[14] Z. H. Sun, *On the theory of cubic residues and non-residues*, Acta Arith. **84** (1998), 291–335.
[15] ———, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361–377.
[16] Surjit Singh and Rajwade, *The number of solutions of the congruence* $y^2 \equiv x^4 - a \pmod{p}$, L'Enseignement Math. (1974), 265–263.
[17] A. Weil, *Number of solutions of equations in a finite field*, Bull. Amer. Math. Soc. **55** (1949), 497–508.
[18] K. S. Williams, *A quadratic partition of primes* $\equiv 1 \pmod{7}$, Math. Comp. **28** (1974), 1133–1136.
[19] ———, *Elementary treatment of quadratic partition of primes* $\equiv 1 \pmod{7}$, Illinois J. Math. **18** (1974), 608–621.

Daeyeoul Kim
Department of Mathematics
Chonbuk National University
Chonju 561-756, Korea
E-mail: dykim@math.chonbuk.ac.kr

Ja Kyung Koo
Department of Mathematics
Korea Advanced Institute of Science and Technology
Tajeon 305-701, Korea
E-mail: jkkoo@math.kaist.ac.kr

Myung-Hwan Kim
Department of Mathematical Science
Seoul National Univ.
Seoul 151-747, Korea
E-mail: mhkim@math.snu.ac.kr