THE CUBIC CONGRUENCE $x^3+ax^2+bx+c\equiv 0(\mathrm{mod}\, p)$ AND BINARY QUADRATIC FORMS $F(x,y)=ax^2+bxy+cy^2$

AHMET TEKCAN

ABSTRACT. Let $F(x,y)=ax^2+bxy+cy^2$ be a binary quadratic form of discriminant $\Delta=b^2-4ac$ for $a,b,c\in\mathbb{Z}$, let p be a prime number and let $\mathbb{F}_p$ be a finite field. In this paper we formulate the number of integer solutions of cubic congruence $x^3+ax^2+bx+c\equiv 0\ (\mathrm{mod}\, p)$ over $\mathbb{F}_p$ for two specific binary quadratic forms $F_1^k(x,y)=x^2+kxy+ky^2$ and $F_2^k(x,y)=kx^2+kxy+k^2y^2$ for integer k such that $1\leq k\leq 9$. Later we consider representation of primes by F_1^k and F_2^k.

AMS Subject Classification 2000: 11D25, 11D79, 11E16, 11E25.
Keywords: Binary quadratic form, cubic congruence, cubic residue, representation of primes by binary quadratic forms.
Date: 29.01.2007.

1. INTRODUCTION.

In 1896, Voronoi [19] presented his algorithm for computing a system of fundamental units of a cubic number field. His technique, described in terms of binary quadratic forms. A real binary quadratic form F is a polynomial in two variables x and y of the type $F=F(x,y)=ax^2+bxy+cy^2$ with real coefficients a,b,c. The discriminant of F is defined by the formula b^2-4ac and is denoted by $\Delta=\Delta(F)$. F is an integral form if and only if $a,b,c\in\mathbb{Z}$, and is indefinite if and only if $\Delta(F)>0$ (for further details on binary quadratic forms see [2,4,10]). Later his technique was restarted in the language of multiplicative lattices by Delone and Faddeev [7]. In 1985, Buchmann [3] generalized the Voronoi's algorithm.

Recall that a cubic congruence over a field $\mathbb{F}_p$ is

$$x^3+ux^2+vx+w\equiv 0(\mathrm{mod}\, p), \tag{1.1}$$

where $u,v,w\in\mathbb{F}_p$ and p is prime. Solutions of cubic congruence (including cubic residues) was considered by many authors. Dietmann [8] consider the

small solutions of additive cubic congruences. Manin [13] consider the cubic congruence on prime modules. Mordell [14,15] consider the cubic congruence in three variables and also the congruence $ax^3+by^3+cz^3+dxyz \equiv n(\mathrm{mod}\, p)$. Williams and Zarnke [20] give some algorithms for solving the cubic congruence on prime modules.

Let $H(\Delta)$ denote the group of classes of primitive, integral binary quadratic forms $F(x,y) = ax^2+bxy+cy^2$ of discriminant Δ. Let K be a quadratic field $\mathbb{Q}(\sqrt{\Delta})$, let L be the splitting field of x^3+ax^2+bx+c, let $f_0 = f_0(L/K)$ be the part of the conductor of the extension L/K and let f be a positive integer with $f_0|f$. In [18], Spearman and Williams consider the cubic congruence $x^3+ax^2+bx+c \equiv 0(\mathrm{mod}\, p)$ and binary quadratic forms $F(x,y) = ax^2+bxy+cy^2$. They proved that the cubic congruence $x^3+ax^2+bx+c \equiv 0(\mathrm{mod}\, p)$ has three solutions if and only if p is represented by a quadratic form F in J, where $J = J(L,K,F)$ is a subgroup of index 3 in $H(\Delta(K)f^2)$.

2. THE CUBIC CONGRUENCE $x^3+ax^2+bx+c \equiv 0(mod\, p)$ AND $F(x,y) = ax^2+bxy+cy^2$.

Let p be a prime number, $\mathbb{F}_p$ be a finite field and let Q_p denote the set of quadratic residues in $\mathbb{F}_p$. In this paper, we consider the solutions of the cubic congruence $x^3+ax^2+bx+c \equiv 0(\mathrm{mod}\, p)$ for given any binary quadratic form $F(x,y) = ax^2+bxy+cy^2$.

Let k be a positive integer such that $1 \le k \le 9$ and let

$$F_1^k(x,y) = x^2+kxy+ky^2 \tag{2.1}$$

be a binary quadratic form. Then the corresponding cubic congruence over $\mathbb{F}_p$ is

$$C_1^k : x^3+x^2+kx+k \equiv 0 \ (\mathrm{mod} p). \tag{2.2}$$

Set

$$\#C_1^k(\mathbb{F}_p) = \left\{x \in \mathbb{F}_p : x^3+x^2+kx+k \equiv 0 \ (\mathrm{mod} p)\right\}.$$

Then we have the following theorem.

Theorem 2.1. *Let C_1^k be a cubic congruence over $\mathbb{F}_p$.*

(1) *If $p \equiv 1(\mathrm{mod}\, 4)$, then $\#C_1^1(\mathbb{F}_p) = 3$, if $p \equiv 3(\mathrm{mod}\, 4)$, then $\#C_1^1(\mathbb{F}_p) = 1$.*

(2) *If $p \equiv 1,3(\mathrm{mod}\, 8)$, then $\#C_1^2(\mathbb{F}_p) = 3$, if $p \equiv 5,7(\mathrm{mod}\, 8)$, then $\#C_1^2(\mathbb{F}_p) = 1$.*

(3) *If* $p \equiv 1, 7 (\mathrm{mod}\, 12)$, *then* $\#C_1^3(\mathbb{F}_p) = 3$ *and if* $p \equiv 5, 11 (\mathrm{mod}\, 12)$, *then* $\#C_1^3(\mathbb{F}_p) = 1$.

(4) *If* $p = 5$, *then* $\#C_1^4(\mathbb{F}_5) = 2$, *if* $p \equiv 1, 5 (\mathrm{mod}\, 12)$, *then* $\#C_1^4(\mathbb{F}_p) = 3$ *and if* $p \equiv 7, 11 (\mathrm{mod}\, 12)$, *then* $\#C_1^4(\mathbb{F}_p) = 1$.

(5) *If* $p \equiv 1, 3, 7, 9 (\mathrm{mod}\, 20)$, *then* $\#C_1^5(\mathbb{F}_p) = 3$, *if* $p \equiv 11, 13, 17, 19 (\mathrm{mod}\, 20)$, *then* $\#C_1^5(\mathbf{F}_p) = 1$.

(6) *If* $p = 7$, *then* $\#C_1^6(\mathbb{F}_7) = 2$, *if* $p \equiv 1, 5, 7, 11, 25, 29, 31, 35 (\mathrm{mod}\, 48)$, *then* $\#C_1^6(\mathbf{F}_p) = 3$ *and if* $p \equiv 13, 17, 19, 23, 37, 41, 43, 47 (\mathrm{mod}\, 48)$, *then* $\#C_1^6(\mathbb{F}_p) = 1$.

(7) *If* $p \equiv 1, 9, 11, 15, 23, 25 (\mathrm{mod}\, 28)$, *then* $\#C_1^7(\mathbb{F}_p) = 3$, *if* $p \equiv 3, 5, 13, 17, 19, 27 (\mathrm{mod}\, 28)$, *then* $\#C_1^7(\mathbb{F}_p) = 1$.

(8) *If* $p \equiv 1, 11, 17, 19, 25, 35, 41, 43 (\mathrm{mod}\, 48)$, *then* $\#C_1^8(\mathbb{F}_p) = 3$, *if* $p \equiv 5, 7, 13, 23, 29, 31, 37, 47 (\mathrm{mod}\, 48)$, *then* $\#C_1^8(\mathbb{F}_p) = 1$.

(9) *If* $p = 5$, *then* $\#C_1^9(\mathbb{F}_5) = 2$, *if* $p \equiv 1, 5, 13, 17 (\mathrm{mod}\, 24)$, *then* $\#C_1^9(\mathbb{F}_p) = 3$ *and if* $p \equiv 7, 11, 19, 23 (\mathrm{mod}\, 24)$, *then* $\#C_1^9(\mathbb{F}_p) = 1$.

Proof. Now consider the cubic congruence $C_1^k : x^3 + x^2 + kx + k \equiv 0 (\mathrm{mod}\, p)$. Then we have

$$\begin{aligned} C_1^k : x^3 + x^2 + kx + k &\equiv 0 (\mathrm{mod}\, p) \\ &\Leftrightarrow x^2(x+1) + k(x+1) \equiv 0 (\mathrm{mod}\, p) \\ &\Leftrightarrow (x+1)(x^2+k) \equiv 0 (\mathrm{mod}\, p). \end{aligned}$$

(1) Let $k = 1$. Then we have $C_1^1 : x^3 + x^2 + x + 1 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow x + 1 \equiv 0 (\mathrm{mod}\, p)$ and $x^2 + 1 \equiv 0 (\mathrm{mod}\, p)$. Hence $x = -1 = p - 1$ is a solution of C_1^1. If $p \equiv 1 (\mathrm{mod}\, 4)$, then the quadratic congruence $x^2 + 1 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow x^2 \equiv -1 (\mathrm{mod}\, p)$ has two solutions since $-1 \in Q_p$. Hence there are total three solutions of C_1^1. If $p \equiv 3 (\mathrm{mod}\, 4)$, then the quadratic congruence $x^2 + 1 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow x^2 \equiv -1 (\mathrm{mod}\, p)$ has no solution since $-1 \notin Q_p$. Hence there are total one solution of C_1^1.

(2) Let $k = 2$. Then

$$C_1^2 : x^3 + x^2 + 2x + 2 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow (x+1)(x^2+2) \equiv 0 (\mathrm{mod}\, p).$$

Hence $x = -1 = p - 1$ is a solution of C_2. If $p \equiv 1, 3 (\mathrm{mod}\, 8)$, then the quadratic congruence $x^2 + 2 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow x^2 \equiv -2 (\mathrm{mod}\, p)$ has two solutions since $-2 \in Q_p$. Hence there are total three solutions of C_1^2. If $p \equiv 5, 7 (\mathrm{mod}\, 8)$, then the quadratic congruence $x^2 + 2 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow x^2 \equiv -2 (\mathrm{mod}\, p)$ has no solution since $-2 \notin Q_p$. Hence there are total one solution of C_1^2.

Now we only prove the special case, that is, the case $\#C_1^k(\mathbb{F}_p) = 2$, because the others can be proved as in the same way that (1) and (2) were proved since

(2.3)
$$\begin{aligned}
p \equiv 1,7 (\mathrm{mod}\, 12) &\Leftrightarrow -3 \in Q_p \\
p \equiv 5,11 (\mathrm{mod}\, 12) &\Leftrightarrow -3 \notin Q_p \\
p \equiv 1,5 (\mathrm{mod}\, 12) &\Leftrightarrow -4 \in Q_p \\
p \equiv 7,11 (\mathrm{mod}\, 12) &\Leftrightarrow -4 \notin Q_p \\
p \equiv 1,3,7,9 (\mathrm{mod}\, 20) &\Leftrightarrow -5 \in Q_p \\
p \equiv 11,13,17,19 (\mathrm{mod}\, 20) &\Leftrightarrow -5 \notin Q_p \\
p \equiv 1,5,7,11,25,29,31,35 (\mathrm{mod}\, 48) &\Leftrightarrow -6 \in Q_p \\
p \equiv 13,17,19,23,37,41,43,47 (\mathrm{mod}\, 48) &\Leftrightarrow -6 \notin Q_p \\
p \equiv 1,9,11,15,23,25 (\mathrm{mod}\, 28) &\Leftrightarrow -7 \in Q_p \\
p \equiv 3,5,13,17,19,27 (\mathrm{mod}\, 28) &\Leftrightarrow -7 \notin Q_p \\
p \equiv 1,11,17,19,25,35,41,43 (\mathrm{mod}\, 48) &\Leftrightarrow -8 \in Q_p \\
p \equiv 5,7,13,23,29,31,37,47 (\mathrm{mod}\, 48) &\Leftrightarrow -8 \notin Q_p \\
p \equiv 1,5,13,17 (\mathrm{mod}\, 24) &\Leftrightarrow -9 \in Q_p \\
p \equiv 7,11,19,23 (\mathrm{mod}\, 24) &\Leftrightarrow -9 \notin Q_p.
\end{aligned}$$

(4) Let $p = 5$. Then

$$C_1^4 : x^3 + x^2 + 4x + 4 \equiv 0 (\mathrm{mod}\, 5) \Leftrightarrow (x+1)(x^2+4) \equiv 0 (\mathrm{mod}\, 5).$$

Hence we get $x = 4$ from $x + 1 \equiv 0 (\mathrm{mod}\, 5)$ and we get $x = 1, 4$ from $x^2 + 4 \equiv 0 (\mathrm{mod}\, 5)$. Therefore there are two integer solutions $x = 1, 4$ of C_1^4 over $\mathbb{F}_5$, that is, $\#C_1^4(\mathbb{F}_5) = 2$.

(6) Let $p = 7$. Then

$$C_1^6 : x^3 + x^2 + 6x + 6 \equiv 0 (\mathrm{mod}\, 7) \Leftrightarrow (x+1)(x^2+6) \equiv 0 (\mathrm{mod}\, 7).$$

Hence we get $x = 6$ from $x + 1 \equiv 0 (\mathrm{mod}\, 7)$ and we get $x = 1, 6$ from $x^2 + 6 \equiv 0 (\mathrm{mod}\, 7)$. Therefore there are two integer solutions $x = 1, 6$ of C_1^6 over $\mathbb{F}_7$.

(9) Let $p = 5$. Then

$$C_1^9 : x^3 + x^2 + 9x + 9 \equiv 0 (\mathrm{mod}\, 5) \Leftrightarrow (x+1)(x^2+9) \equiv 0 (\mathrm{mod}\, 5).$$

Hence we get $x = 4$ from $x + 1 \equiv 0 (\mathrm{mod}\, 5)$ and we get $x = 1, 4$ from $x^2 + 9 \equiv 0 (\mathrm{mod}\, 5)$. Therefore there are two integer solutions $x = 1, 4$ of C_1^9 over $\mathbb{F}_5$. □

Let k be a positive integer such that $1 \leq k \leq 9$ and let

(2.4)
$$F_2^k(x, y) = kx^2 + kxy + k^2y^2$$

be a binary quadratic form. Then the corresponding cubic congruence is

$$C_2^k : x^3 + kx^2 + kx + k^2 \equiv 0 (\mathrm{mod}\, p) \tag{2.5}$$

over $\mathbb{F}_p$. Set

$$\#C_2^k(\mathbb{F}_p) = \left\{ x \in \mathbb{F}_p : x^3 + kx^2 + kx + k^2 \equiv 0 (\mathrm{mod}\, p) \right\}.$$

Then we have the following theorem.

Theorem 2.2. *Let C_2^k be a cubic congruence over $\mathbb{F}_p$.*

(1) *If $p \equiv 1 (\mathrm{mod}\, 4)$, then $\#C_2^1(\mathbb{F}_p) = 3$ and if $p \equiv 3 (\mathrm{mod}\, 4)$, then $\#C_2^1(\mathbb{F}_p) = 1$.*

(2) *If $p \equiv 1, 3 (\mathrm{mod}\, 8)$, then $\#C_2^2(\mathbb{F}_p) = 3$ and if $p \equiv 5, 7 (\mathrm{mod}\, 8)$, then $\#C_2^2(\mathbb{F}_p) = 1$.*

(3) *If $p \equiv 1, 7 (\mathrm{mod}\, 12)$, then $\#C_2^3(\mathbb{F}_p) = 3$ and if $p \equiv 5, 11 (\mathrm{mod}\, 12)$, then $\#C_2^3(\mathbb{F}_p) = 1$.*

(4) *If $p = 5$, then $\#C_2^4(\mathbb{F}_5) = 2$, if $p \equiv 1, 5 (\mathrm{mod}\, 12)$, then $\#C_2^4(\mathbb{F}_p) = 3$ and if $p \equiv 7, 11 (\mathrm{mod}\, 12)$, then $\#C_2^4(\mathbb{F}_p) = 1$.*

(5) *If $p \equiv 1, 3, 7, 9 (\mathrm{mod}\, 20)$, then $\#C_2^5(\mathbb{F}_p) = 3$, if $p \equiv 11, 13, 17, 19 (\mathrm{mod}\, 20)$, then $\#C_2^5(\mathbb{F}_p) = 1$.*

(6) *If $p = 7$, then $\#C_2^6(\mathbb{F}_7) = 2$, if $p \equiv 1, 5, 7, 11, 25, 29, 31, 35 (\mathrm{mod}\, 48)$, then $\#C_2^6(\mathbb{F}_p) = 3$ and if $p \equiv 13, 17, 19, 23, 37, 41, 43, 47 (\mathrm{mod}\, 48)$, then $\#C_2^6(\mathbb{F}_p) = 1$.*

(7) *If $p \equiv 1, 9, 11, 15, 23, 25 (\mathrm{mod}\, 28)$, then $\#C_2^7(\mathbb{F}_p) = 3$, if $p \equiv 3, 5, 13, 17, 19, 27 (\mathrm{mod}\, 28)$, then $\#C_2^7(\mathbb{F}_p) = 1$.*

(8) *If $p \equiv 1, 11, 17, 19, 25, 35, 41, 43 (\mathrm{mod}\, 48)$, then $\#C_2^8(\mathbb{F}_p) = 3$ and if $p \equiv 5, 7, 13, 23, 29, 31, 37, 47 (\mathrm{mod}\, 48)$, then $\#C_2^8(\mathbb{F}_p) = 1$.*

(9) *If $p = 5$, then $\#C_2^9(\mathbb{F}_5) = 2$, if $p \equiv 1, 5, 13, 17 (\mathrm{mod}\, 24)$, then $\#C_2^9(\mathbb{F}_p) = 3$ and if $p \equiv 7, 11, 19, 23 (\mathrm{mod}\, 24)$, then $\#C_2^9(\mathbb{F}_p) = 1$.*

Proof. Now consider the cubic congruence $C_2^k : x^3 + kx^2 + kx + k^2 \equiv 0 (\mathrm{mod}\, p)$. Then we have

$$\begin{aligned} C_2^k : x^3 + kx^2 + kx + k^2 &\equiv 0 (\mathrm{mod}\, p) \\ &\Leftrightarrow x^2(x+k) + k(x+k) \equiv 0 (\mathrm{mod}\, p) \\ &\Leftrightarrow (x+k)(x^2+k) \equiv 0 (\mathrm{mod}\, p). \end{aligned}$$

Hence we have $x = p - k$ and $x^2 + k \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow x^2 \equiv -k (\mathrm{mod}\, p)$. So the quadratic congruence $x^2 \equiv -k (\mathrm{mod}\, p)$ has two solutions if $-k \in Q_p$ and has no solution if $-k \notin Q_p$. We know from (2.3) that for which primes p, $-k$ is a quadratic residue and for which primes it is not. So we only prove the other cases.

(4) Let $p = 5$. Then

$$C_2^4 : x^3 + 4x^2 + 4x + 16 \equiv 0(\mathrm{mod}\, 5) \Leftrightarrow (x+4)(x^2+4) \equiv 0(\mathrm{mod}\, 5).$$

Hence we get $x = 1$ from $x + 4 \equiv 0(\mathrm{mod}\, 5)$ and we get $x = 1, 4$ from $x^2 + 4 \equiv 0(\mathrm{mod}\, 5)$. Therefore there are two integer solutions $x = 1, 4$ of C_2^4 over $\mathbb{F}_5$.

(6) Let $p = 7$. Then

$$C_2^6 : x^3 + 6x^2 + 6x + 36 \equiv 0(\mathrm{mod}\, 7) \Leftrightarrow (x+6)(x^2+6) \equiv 0(\mathrm{mod}\, 7).$$

Hence we get $x = 1$ from $x + 6 \equiv 0(\mathrm{mod}\, 7)$ and we get $x = 1, 6$ from $x^2 + 6 \equiv 0(\mathrm{mod}\, 7)$. Therefore there are two integer solutions $x = 1, 6$ of C_2^6 over $\mathbb{F}_7$.

(9) Let $p = 5$. Then

$$C_2^9 : x^3 + 9x^2 + 9x + 81 \equiv 0(\mathrm{mod}\, 5) \Leftrightarrow (x+9)(x^2+9) \equiv 0(\mathrm{mod}\, 5).$$

Hence we get $x = 1$ from $x + 9 \equiv 0(\mathrm{mod}\, 5)$ and we get $x = 1, 4$ from $x^2 + 9 \equiv 0(\mathrm{mod}\, 5)$. Therefore there are two integer solutions $x = 1, 4$ of C_2^9 over $\mathbb{F}_5$. □

3. Representation of Primes by Binary Quadratic Forms.

Representation of integers (or primes) by binary quadratic forms has an important role on the theory of numbers and many authors consider this problem [5,11,12,16,17]. In fact, this problem intimately connected to reciprocity laws [6]. The major problem of the theory of quadratic forms was: Given a form F, find all integers n that can be represented by F, that is, for which $F(x, y) = ax^2 + bxy + cy^2 = n$. This problem was studied for specific quadratic forms by Fermat, and intensively investigated by Euler. Fermat considered the representation of integers as sums of two squares. It was, however, Gauss in the Disquisitiones who made the fundamental breakthrough and developed a comprehensive and beautiful theory of binary quadratic forms. Most important was his definition of the composition of two forms and his proof that the (equivalence classes of) forms with a given discriminant Δ form a commutative group under this composition. The idea behind composition of forms is simple. If forms F and G represent integers n and m, respectively, then their composition $F * G$ [10, p.149] should represent $n.m$. The implementation of this idea is subtle and extremely difficult to describe [9]. Attempts to gain conceptual insight into Gauss theory of composition of forms inspired the efforts of some of the best mathematicians of the time, among them Dirichlet, Kummer and Dedekind. The main ideal here was to extend the domain of higher arithmetic and view the problem in a broader context. Note that the equation

$F(x,y) = ax^2 + bxy + cy^2 = n$ can be rewritten as

$$\begin{aligned} F(x,y) &= ax^2 + bxy + cy^2 \\ &= \frac{1}{a}\left(ax + \frac{b+\sqrt{\Delta}}{2}y\right)\left(ax + \frac{b-\sqrt{\Delta}}{2}y\right) \\ &= n. \end{aligned}$$

Therefore we have thus expressed the problem of representation of integers by binary quadratic forms in terms of domain

$$R = \left\{ \frac{u + v\sqrt{\Delta}}{2} : u, v \in \mathbb{Z}, u \equiv v (\mathrm{mod}\, 2) \right\}.$$

So if we take $a = \alpha$ and $b = \frac{b+\sqrt{\Delta}}{2}$, then we have

$$ax^2 + bxy + cy^2 = \frac{1}{a}(\alpha x + \beta y)(\overline{\alpha} x + \overline{\beta} y) = \frac{1}{a} N(\alpha x + \beta y),$$

where N denotes the norm. Thus to solve $F(x,y) = m$ is to find $x, y \in \mathbb{Z}$ such that $N(\alpha x + \beta y) = m$. Kummer noted in 1840 that the entire theory of binary quadratic forms can be regarded as the theory of complex numbers of the form $x + y\sqrt{\Delta}$ [1, p.585].

In this section we will consider the representation of primes by binary quadratic forms $F_1^k = (1, k, k)$ and $F_2^k = (k, k, k^2)$ for $1 \leq k \leq 9$.

Theorem 3.1. *Let $F_1^k(x,y) = x^2 + kxy + ky^2$. Then*

(1) *Every prime number $p \equiv 1 (\mathrm{mod}\, 6)$ can be represented by F_1^1.*
(2) *Every prime number $p \equiv 1, 5 (\mathrm{mod}\, 8)$ can be represented by F_1^2.*
(3) *Every prime number $p \equiv 1 (\mathrm{mod}\, 6)$ can be represented by F_1^3.*
(4) *There is no prime number can be represented by F_1^4.*
(5) *Every prime number $p \equiv 1, 5, 9, 11, 19 (\mathrm{mod}\, 20)$ can be represented by F_1^5.*
(6) *Every prime number $p \equiv 1 (\mathrm{mod}\, 12)$ can be represented by F_1^6.*
(7) *Every prime number $p \equiv 1, 7, 25, 37 (\mathrm{mod}\, 42)$ can be represented by F_1^7.*
(8) *Every prime number $p \equiv 1, 9 (\mathrm{mod}\, 16)$ can be represented by F_1^8.*
(9) *Every prime number $p \equiv 1, 19 (\mathrm{mod}\, 30)$ can be represented by F_1^9.*

Proof. (1) Let p be a prime number such that $p \equiv 1 (\mathrm{mod}\, 6)$. Note that the discriminant of $F_1^1(x,y) = x^2 + xy + y^2$ is -3, that is, $\Delta(F_1^1) = -3$, and also the class number for this discriminant is -1 [10, p.194]. Therefore every prime number $p \equiv 1 (\mathrm{mod}\, 6)$ can be represented by F_1^1. In other words, the ring of integers in the field generated by a square root of -3 is a PID. Since

primes $p \equiv 1 (\mathrm{mod}\, 3)$ split there, we have $(p) = P\overline{P}$. Let $P = x + yw$, where $w^2 + w + 1 = 0$. Then if we take norm, then we have the result.

Now we only prove (4) since the others can be proved as in the same way that (1) was proved. Let p be a arbitrary prime number. Then the Diophantine equation

$$F_1^4(x, y) = x^2 + 4y + 4y^2 = (x + 2y)^2 = p$$

has no solution (x, y) since p is prime. □

Theorem 3.2. *Let* $F_2^k(x, y) = kx^2 + kxy + k^2y^2$. *Then*

(1) *Every prime number* $p \equiv 1 (\mathrm{mod}\, 6)$ *can be represented by* F_2^1.
(2) *There is no prime number can be represented by* F_2^2.
(3) *There is no prime number can be represented by* F_2^3.
(4) *There is no prime number can be represented by* F_2^4.
(5) *There is no prime number except for* $p = 5$ *can be represented by* F_2^5.
(6) *There is no prime number can be represented by* F_2^6.
(7) *There is no prime number except for* $p = 7$ *can be represented by* F_2^7.
(8) *There is no prime number can be represented by* F_2^8.
(9) *There is no prime number can be represented by* F_2^9.

Proof. (1) Let $k = 1$. Then $F_2^1(x, y) = x^2 + xy + y^2 = F_1^1(x, y)$ which is the binary quadratic form in (1) of Theorem 3.1. Therefore every prime number $p \equiv 1 (\mathrm{mod}\, 6)$ can be represented by F_2^1.

(2) Let $k = 2$ and let p can be represented by F_2^2. Then the equation

$$\begin{aligned} F_2^2(x, y) &= 2x^2 + 2xy + 4y^2 = p \\ &\Leftrightarrow 2x^2 + 2xy + 4y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-y \pm \sqrt{2p - 7y^2}}{2} \end{aligned}$$

has an integer solution (x, y). So $2p - 7y^2$ must be a square. Let $2p - 7y^2 = t^2$ for a non zero integer t. Then

$$p = \frac{t^2 + 7y^2}{2}$$

must be a prime. If t is odd and y is even or t is even and y is odd, then $\frac{t^2+7y^2}{2}$ is rational, if t and y both even or odd, then $\frac{t^2+7y^2}{2}$ is even. Therefore in both cases $\frac{t^2+7y^2}{2}$ can not be a prime number, which is a contradiction. Consequently, the equation $F_2^2(x, y) = 2x^2 + 2xy + 4y^2 = p$ has no integer solution, that is, there is no prime p can be represented by F_2^2.

(3) Let $k = 3$ and let p can be represented by F_2^3. Then the equation

$$\begin{aligned} F_2^3(x,y) &= 3x^2 + 3xy + 9y^2 = p \\ &\Leftrightarrow 3x^2 + 3xy + 9y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-3y \pm \sqrt{12p - 99y^2}}{6} \end{aligned}$$

has an integer solution (x, y). So $12p - 99y^2$ must be a square. Let $12p - 99y^2 = t^2$. Then

$$p = \frac{t^2 + 99y^2}{12}$$

must be a prime. Note that $\frac{t^2+99y^2}{12}$ is odd if t is an odd multiple of 3 and y is odd, is even or odd if t is an even multiple of 3 and y is even and is rational otherwise. So if $\frac{t^2+99y^2}{12}$ is even or rational, then it can not be a prime. We know that $\frac{t^2+99y^2}{12}$ is odd if t is an odd multiple of 3 and y is odd or t is an even multiple of 3 and y is even. So if t is an odd multiple of 3 and y is odd, then $x_{1,2} = \frac{-3y \pm t}{6} = \frac{-y}{2} \pm \frac{t}{6}$ is not an integer. If t is an even multiple of 3 and y is even, then $x_{1,2} = \frac{-3y \pm t}{6} = \frac{-y}{2} \pm \frac{t}{6}$ is an integer but in this case $\frac{t^2+99y^2}{12}$ is not a prime. So in all cases there is no integer solutions, that is, there is no prime p can be represented by F_2^3.

(4) Let $k = 4$ and let p can be represented by F_2^4. Then the equation

$$\begin{aligned} F_2^4(x,y) &= 4x^2 + 4xy + 16y^2 = p \\ &\Leftrightarrow 4x^2 + 4xy + 16y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-y \pm \sqrt{p - 15y^2}}{2} \end{aligned}$$

has an integer solution (x, y). So $p - 15y^2$ must be a square. Let $p - 15y^2 = t^2$. Then

$$p = t^2 + 15y^2$$

must be a prime. If t and y are both even or odd, then $t^2 + 15y^2$ is even, and if t is odd and y is even, or t is even and y is odd, then $t^2 + 15y^2$ is odd. If $t^2 + 15y^2$ is even, then it can not be a prime. If $t^2 + 15y^2$ is odd, then we know that t is odd and y is even or t is even and y is odd. So in both cases $x_{1,2} = \frac{-y}{2} \pm \frac{t}{2}$ is not an integer. Consequently, there is no integer solution of $F_2^4(x,y) = 4x^2 + 4xy + 16y^2 = p$.

(5) Let $k = 5$. First we show that 5 can be represented by F_2^5. It is easily seen that the equation

$$F_2^5(x,y) = 5x^2 + 5xy + 25y^2 = 5$$

has integer solutions $(\pm 1, 0)$. Therefore 5 can be represented by F_2^5.

Let $p > 5$ can be represented by F_2^5. Then the equation

$$\begin{aligned} F_2^5(x,y) &= 5x^2 + 5xy + 25y^2 = p \\ &\Leftrightarrow 5x^2 + 5xy + 25y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-5y \pm \sqrt{20p - 475y^2}}{10} \end{aligned}$$

has an integer solution (x, y). So $20p - 475y^2$ must be a square. Let $20p - 475y^2 = t^2$. Then

$$p = \frac{t^2 + 475y^2}{20}$$

must be a prime. Note that $\frac{t^2+475y^2}{20}$ is odd if t is an odd multiple of 5 and y is odd, is even or odd if t is an even multiple of 5 and y is even and is rational otherwise. So if $\frac{t^2+475y^2}{20}$ is even or rational, then it can not be a prime. If $\frac{t^2+475y^2}{20}$ is odd, then we know that t is an odd multiple of 5 and y is odd or t is an even multiple of 5 and y is even. If t is an odd multiple of 5 and y is odd, then $\frac{t^2+475y^2}{20}$ is divisible by 5, and if t is an even multiple of 5 and y is even, then $\frac{t^2+475y^2}{20}$ is divisible by 5. So it both cases it can not be a prime. Therefore the equation $F_2^5(x,y) = 5x^2 + 5xy + 25y^2 = p$ has no solution (x, y).

(6) Let $k = 6$ and let p can be represented by F_2^6. Then the equation

$$\begin{aligned} F_2^6(x,y) &= 6x^2 + 6xy + 36y^2 = p \\ &\Leftrightarrow 6x^2 + 6xy + 36y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-3y \pm \sqrt{6p - 207y^2}}{6} \end{aligned}$$

has an integer solution (x, y). So Let $6p - 207y^2$ must be a square. Let $6p - 207y^2 = t^2$. Then

$$p = \frac{t^2 + 207y^2}{6}$$

must be a prime. Note that $\frac{t^2+207y^2}{6}$ is even if t is an odd multiple of 3 and y is odd or if t is an even multiple of 3 and y is even and is rational otherwise. In both cases it can not be a prime. Therefore the equation $F_2^6(x,y) = 6x^2 + 6xy + 36y^2 = p$ has no integer solution.

(7) Let $k = 7$. First we show that 7 can be represented by F_2^7. It is easily seen that the equation

$$F_2^7(x,y) = 7x^2 + 7xy + 49y^2 = 7$$

has integer solutions $(\pm 1, 0)$. Therefore 7 can be represented by F_2^7.

Let $p > 7$ can be represented by F_2^7. Then the equation

$$\begin{aligned} F_2^7(x,y) &= 7x^2 + 7xy + 49y^2 = p \\ &\Leftrightarrow 7x^2 + 7xy + 49y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-7y \pm \sqrt{28p - 1323y^2}}{14} \end{aligned}$$

has an integer solution (x, y). So $28p - 1323y^2$ must be a square. Let $28p - 1323y^2 = t^2$. Then

$$p = \frac{t^2 + 1323y^2}{28}$$

must be a prime. Note that $\frac{t^2+1323y^2}{28}$ is odd if t is an odd multiple of 7 and y is odd, is even or odd if t is an even multiple of 7 and y is even and is rational otherwise. So if $\frac{t^2+1323y^2}{28}$ is even or rational, then it can not be a prime. If $\frac{t^2+1323y^2}{28}$ is odd, then we know that if t is an odd multiple of 7 and y is odd or t is an even multiple of 7 and y is even. So if t is an odd multiple of 7 and y is odd, then $x_{1,2} = \frac{-7y \pm t}{14} = \frac{-y}{2} \pm \frac{t}{14}$ is not an integer. If t is an even multiple of 7 and y is even, then $x_{1,2} = \frac{-7y \pm t}{14} = \frac{-y}{2} \pm \frac{t}{14}$ is an integer but in this case $\frac{t^2+1323y^2}{28}$ is not a prime. So in all cases the equation $F_2^7(x,y) = 7x^2 + 7xy + 49y^2 = p$ has no integer solution (x, y).

(8) Let $k = 8$ and let p can be represented by F_2^8. Then the equation

$$\begin{aligned} F_2^8(x,y) &= 8x^2 + 8xy + 64y^2 = p \\ &\Leftrightarrow 8x^2 + 8xy + 64y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-2y \pm \sqrt{2p - 124y^2}}{4} \end{aligned}$$

has an integer solution (x, y). So $2p - 124y^2$ must be a square. Let $2p - 124y^2 = t^2$. Then

$$p = \frac{t^2 + 124y^2}{2}$$

must be a prime. If t is even, then $\frac{t^2+124y^2}{2}$ is even and if t is odd, then $\frac{t^2+124y^2}{2}$ is rational. So in both cases, it can not be a prime. Therefore the equation $F_2^8(x,y) = 8x^2 + 8xy + 64y^2 = p$ has no integer solution.

(9) Let $k = 9$ and let p can be represented by F_2^9. Then the equation

$$\begin{aligned} F_2^9(x,y) &= 9x^2 + 9xy + 81y^2 = p \\ &\Leftrightarrow 9x^2 + 9xy + 81y^2 - p = 0 \\ &\Leftrightarrow x_{1,2} = \frac{-9y \pm \sqrt{36p - 2835y^2}}{18} \end{aligned}$$

has an integer solution (x, y). So $36p - 2835y^2$ be a square. Let $36p - 2835y^2 = t^2$. Then

$$p = \frac{t^2 + 2835y^2}{36}$$

must be a prime. Note that $\frac{t^2+2835y^2}{36}$ is odd if t is an odd multiple of 3 and y is odd, is even or odd if t is an even multiple of 3 and y is even and is rational otherwise. So if $\frac{t^2+2835y^2}{36}$ is even or rational, then it can not be a prime. If $\frac{t^2+2835y^2}{36}$ is odd, then we know that t is an odd multiple of 3 and y is odd or t is an even multiple of 3 and y is even. So if t is an odd multiple of 3 and y is odd, then $x_{1,2} = \frac{-9y \pm t}{18} = \frac{-y}{2} \pm \frac{t}{18}$ is not an integer. If t is an even multiple of 3 and y is even, then $x_{1,2} = \frac{-9y \pm t}{18} = \frac{-y}{2} \pm \frac{t}{18}$ is not an integer or an integer but in this case $\frac{t^2+2835y^2}{36}$ is not a prime. So in all cases the equation $F_2^9(x, y) = 9x^2 + 9xy + 81y^2 = p$ has no integer solution. □

REFERENCES

[1] Bourbaki, N. *Historical Note, in his Commutative Algebra.* Addison-Wesley Publ. Co., Reading, MA, 1972.

[2] Buchmann, J. *Algorithms for Binary Quadratic Forms.* In preparation, accepted by Springer-Verlag.

[3] Buchmann, J. *A generalization of Voronoi's Algorithm I,II.* J. Number Theory 20(1985), 177–209.

[4] Buell, D.A. *Binary Quadratic Forms, Clasical Theory and Modern Computations* Springer-Verlag, New York, 1989.

[5] Christofferson, S. *On Representation of Integers by Binary Quadratic Forms in Algebraic Number Fields.* Uppsala : Almqvist & Wiksells Boktryckeri Ab, 1962.

[6] Cox, D.A. *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multilication* John Wiley& Sons, Inc., New York, 1989.

[7] Delone, B.N. and Faddeev, K. *The Theory of Irrationalities of the Third Degree.* Transl. Math. Monographs **10**, Amer. Math. Soc., Providence, Rhode Island 1964.

[8] Dietmann, R. *Small Solutions of Additive Cubic Congruences.* Archiv der Mathematik **75**(3)(2000), 195–197.

[9] Edwards, H.M. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* Springer-Verlag New York, 1977.

[10] Flath, D.E. *Introduction to Number Theory.* Wiley, 1989.

[11] Hudson, R.H. and Williams, K.S. *Congruences for Representation of Primes by Binary Quadratic Forms.* Acta Arith. **41**(1982), 311–322.

[12] Koch, F. H. *Representation of Primes by Binary Quadratic Forms of Discriminant $-256q$ and $-128q$.* Glasgow Math. J. **35**(1993), 261–268.

[13] Manin, Y.I. *On a Cubic Congrunce to a Prime Modules.* Amer. Math. Soc. Transl. **13**(1960), 1–7.

[14] Mordell, L.J. *On a Cubic Congruence in Three Variables, II.* Proc Amer. Math.Soc. 14(4)(1963), 609–614.

[15] Mordell, L.J. *On the Congruence $ax^3 + by^3 + cz^3 + dxyz \equiv n(mod p)$.* Duke Math. J. **31**(1)(1964), 123–126

[16] Muskat, J.B. *On Simultaneous Representations of Primes by Binary Quadratic Forms.* J. Number Theory **19**(1984), 263–282.

[17] Muskat, J.B., Spearman, B.K. and Williams, K. S. *Predictive Criteria for the Representation of Primes by Binary Quadratic Forms.* Acta Arithmetica **LXX**(3)(1995), 215–278.

[18] Spearman, B.K. and Williams, K. *The Cubic Congrunce* $x^3 + Ax^2 + Bx + C \equiv 0 (mod p)$ *and Binary Quadratic Forms II.* J. London Math. Soc. **64**(2)(2001), 273–274.

[19] Voronoi, G.F. *On a Generalization of the Algorithm of Continued Fractions.* (in Russian). Phd Dissertation, Warsaw, 1896.

[20] Williams, H.C. and Zarnke, C.R. *Some Algoritms for Solving a Cubic Congruence modulo p.* Utilitas Mathematica **6**(1974), 285–306.

ULUDAG UNIVERSITY, FACULTY OF SCIENCE, DEPARTMENT OF MATHEMATICS, GÖRÜKLE 16059, BURSA-TURKEY

E-mail address: tekcan@uludag.edu.tr