Acta Universitatis Apulensis No. 22/2010
ISSN: 1582-5329 pp. 53-63

THE CUBIC CONGRUENCE $X^3 + AX^2 + BX + C \equiv 0(MOD\,P)$ AND BINARY QUADRATIC FORMS $F(X, Y) = AX^2 + BXY + CY^2$ II

Ahmet Tekcan

Abstract. Let $F(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form of discriminant $\Delta = b^2 - 4ac$, let $p \geq 5$ be a prime number and let $\mathbf{F}_p$ be a finite field. In the first section, we give some preliminaries from cubic congruence and binary quadratic forms. In the second section, we consider the number of integer solutions of quadratic congruence $x^2 \equiv \pm k(mod\,p)$, where k is an integer such that $1 \leq k \leq 10$. In the third section, we consider the number of integer solutions of cubic congruences $x^3 + ax^2 + bx + c \equiv 0(mod\,p)$ over $\mathbf{F}_p$ for two specific binary quadratic forms $F_1^k(x, y) = 2kx^2 + kxy + 2k^2y^2$ and $F_2^k(x, y) = -3kx^2 - kxy + 3k^2y^2$. In the last section, we consider representation of primes by F_1^k and F_2^k.

2000 *Mathematics Subject Classification*: 11E16, 11E25, 11D25, 11D79.

Keywords and phrases: Binary quadratic form, cubic congruence, representation of primes by quadratic forms.

1. Introduction

In 1896, Voronoi [15] presented his algorithm for computing a system of fundamental units of a cubic number field. His technique, described in terms of binary quadratic forms. Recall that a real binary quadratic form F (or just a form) is a polynomial in two variables x and y of the type

$$F = F(x, y) = ax^2 + bxy + cy^2 \qquad (1)$$

with real coefficients a, b, c. The discriminant of F is defined by the formula $b^2 - 4ac$ and is denoted by $\Delta = \Delta(F)$. If $a, b, c \in \mathbf{Z}$, then F is called integral, and if $gcd(a, b, c) = 1$, then F is called primitive (for further details on binary quadratic forms see [2,4,8]). Later Voronoi's technique was restarted in the language of multiplicative lattices by Delone and Faddeev [5]. In 1985, Buchmann [3] generalized the Voronoi's algorithm.

Let $p \geq 5$ be a prime number. Then a cubic congruence over a finite field $\mathbf{F}_p$ is given by

$$x^3 + ax^2 + bx + c \equiv 0(mod\, p), \tag{2}$$

where $a, b, c \in \mathbf{F}_p$. Solutions of cubic congruence (including cubic residues) were considered by many authors. Dietmann [6] considered the small solutions of additive cubic congruences, Manin [10] considered the cubic congruence on prime modules, Mordell [11,12] considered the cubic congruence in three variables and also the congruence $ax^3 + by^3 + cz^3 + dxyz \equiv n(mod\, p)$, Williams and Zarnke [16] gave 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 of discriminant Δ, let K be a quadratic field $\mathbf{Q}(\sqrt{\Delta})$, 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 [13], Spearman and Williams considered the cubic congruence $x^3 + ax^2 + bx + c \equiv 0(mod\, p)$ and binary quadratic forms $F(x, y) = ax^2 + bxy + cy^2$. They proved that the cubic congruence $x^3 + ax^2 + bx + c \equiv 0(mod\, p)$ 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 $H(\Delta(K)f^2)$. Now we can give the following two Lemmas.

Lemma 1.1. *Let $a \in \mathbf{F}_p$. Then*

$$a^{(p-1)/2} = \begin{cases} 1 & if\ a \in Q_p \\ -1 & if\ a \notin Q_p. \end{cases}$$

In other words $(\frac{a}{p}) = a^{(p-1)/2}$, where $(\frac{\cdot}{p})$ denotes the Legendre symbol and Q_p denotes the set of quadratic residues in $\mathbf{F}_p$.

Lemma 1.2. *Let $a \in \mathbf{F}_p^* = \mathbf{F}_p - \{0\}$ and let $\left\{a, 2a, 3a, \cdots, \frac{p-1}{2}a\right\}$ be the set of multiplies of a. Represent each of these elements of $\mathbf{F}_p$ by an integer in the range $\left(\frac{-p}{2}, \frac{p}{2}\right)$, and let v denote the number of negative integers in this set. Then $(\frac{a}{p}) = (-1)^v$.*

2. The Quadratic Congruence $x^2 \equiv \pm k(mod\, p)$.

In this section, we will consider the quadratic congruence $x^2 \equiv \pm k(mod\, p)$ over finite fields, where k is an integer such that $1 \leq k \leq 10$. We want to determine when this congruence has two solutions or not, that is, when $(\frac{\pm k}{p}) = 1$ or $(\frac{\pm k}{p}) = -1$. First we start with $x^2 \equiv k(mod\, p)$.

Theorem 2.1. *Let $\mathbf{F}_p$ be a finite field. Then*

$$
\begin{aligned}
\left(\frac{1}{p}\right) &= 1\ for\ every\ prime\ p \geq 5\\
\left(\frac{2}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,7(mod\,8)\\ -1 & if\ p \equiv 3,5(mod\,8)\end{cases}\\
\left(\frac{3}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,11(mod\,12)\\ -1 & if\ p \equiv 5,7(mod\,12)\end{cases}\\
\left(\frac{4}{p}\right) &= 1\ for\ every\ prime\ p \geq 5\\
\left(\frac{5}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,9(mod\,10)\\ -1 & if\ p \equiv 3,7(mod\,10)\end{cases}\\
\left(\frac{6}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,5,19,23(mod\,24)\\ -1 & ifp \equiv 7,11,13,17(mod\,24)\end{cases}\\
\left(\frac{7}{p}\right) &= \begin{cases} 1 & ifp \equiv 1,3,9,19,25,27(mod\,28)\\ -1 & if\ p \equiv 5,11,13,15,17,23(mod\,28)\end{cases}\\
\left(\frac{8}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,7,17,23(mod\,24)\\ -1 & if\ p \equiv 5,11,13,19(mod\,24)\end{cases}\\
\left(\frac{9}{p}\right) &= 1\ for\ every\ prime\ p \geq 11\\
\left(\frac{10}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,3,9,13,27,31,37,39(mod\,40)\\ -1 & if\ p \equiv 7,11,17,19,21,23,29,33,37(mod\,40).\end{cases}
\end{aligned}
$$

Proof. Let $p \geq 5$ be any prime number. Then $p-1$ is always even. Hence the first assertion is clear by Lemma 1.1 since $1^{(p-1)/2} = 1$ for all prime $p \geq 5$.

Now we consider the second case, that is, the case $(\frac{2}{p})$. Let us consider the set $\{2,4,6,\cdots,p-1\}$. We know that 2 is an quadratic residue $mod\,p$ if and only if v lie in the interval $(-\frac{p}{2},0)$ is even by Lemma 1.2. Note that v is the number of even integers in the interval $\left[\frac{p+1}{2},p-1\right]$. Let $\frac{p+1}{2}$ is even. Then $p \equiv 3(mod\,4)$ and hence $v = \frac{(p-1)-\frac{p+1}{2}}{2}+1 = \frac{p+1}{4}$. So $\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = 1$ if $p \equiv 7(mod\,8)$ or -1 if $p \equiv 3(mod\,8)$. Similarly let $\frac{p+1}{2}$ is odd. Then $p \equiv 1(mod\,4)$, and hence $v = \frac{(p-1)-\frac{p+3}{2}}{2}+1 = \frac{p-1}{4}$. Therefore $\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = 1$ if $p \equiv 1(mod\,8)$ or -1 if $p \equiv 5(mod\,8)$. Consequently,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & if\ p \equiv 1,7(mod\,8)\\ -1 & if\ p \equiv 3,5(mod\,8).\end{cases}$$

The others can be proved in the same way that $(\frac{2}{p})$ was proved.

Now we consider the quadratic congruence $x^2 \equiv -k(mod\, p)$ for $1 \leq k \leq 10$.

Theorem 2.2. *Let* $\mathbf{F}_p$ *be a finite field. Then*

$$\begin{aligned}
\left(\frac{-1}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1(mod\, 4) \\ -1 & if p \equiv 3(mod\, 4) \end{cases} \\
\left(\frac{-2}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,3(mod\, 8) \\ -1 & if\ p \equiv 5,7(mod\, 8) \end{cases} \\
\left(\frac{-3}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,7(mod\, 12) \\ -1 & if\ p \equiv 5,11(mod\, 12) \end{cases} \\
\left(\frac{-4}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,5(mod\, 12) \\ -1 & if\ p \equiv 7,11(mod\, 12) \end{cases} \\
\left(\frac{-5}{p}\right) &= \begin{cases} 1 & if p \equiv 1,3,7,9(mod\, 20) \\ -1 & if\ p \equiv 11,13,17,19(mod\, 20) \end{cases} \\
\left(\frac{-6}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,5,7,11,25,29,31,35(mod\, 48) \\ -1 & if\ p \equiv 13,17,19,23,37,41,43,47(mod\, 48) \end{cases} \\
\left(\frac{-7}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,9,11,15,23,25(mod\, 28) \\ -1 & if\ p \equiv 3,5,13,17,19,27(mod\, 28) \end{cases} \\
\left(\frac{-8}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,11,17,19,25,35,41,43(mod\, 48) \\ -1 & if\ p \equiv 5,7,13,23,29,31,37,47(mod\, 48) \end{cases} \\
\left(\frac{-9}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,5,13,17(mod\, 24) \\ -1 & if\ p \equiv 7,11,19,23(mod\, 24) \end{cases} \\
\left(\frac{-10}{p}\right) &= \begin{cases} 1 & if\ p \equiv 1,7,9,11,13,19,23,37(mod\, 40) \\ -1 & if\ p \equiv 3,17,21,27,29,31,33,39(mod\, 40). \end{cases}
\end{aligned}$$

Proof. Let $p \equiv 1(mod\, 4)$, say $p = 1 + 4t$ for an integer $t \geq 1$. Then by Lemma 1.1, we get $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2t} = 1$. Similarly it can be shown that when $p \equiv 3(mod\, 4)$, then $(\frac{-1}{p}) = -1$.

Let us consider the set $\{2, 4, 6, \cdots, p-1\}$. We know by Theorem 2.1 that 2 is a quadratic residue $mod\, p$ if and only if v lie in the interval $(-\frac{p}{2}, 0)$ is even. We also proved in above theorem that $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1,7(mod\, 8)$ or -1 if $p \equiv 3,5(mod\, 8)$. Further we see as above that $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1(mod\, 4)$ or -1 if $p \equiv 3(mod\, 4)$.

Combining these two results we conclude that $\left(\frac{-2}{p}\right) = 1$ if $p \equiv 1,3(mod\, 8)$ or -1 if $p \equiv 5,7(mod\, 8)$. The others are similar.

3. Cubic Congruence $x^3 + ax^2 + bx + c \equiv 0(mod\, p)$.

In [14], we consider the number of integer solutions of cubic congruences $x^3 + ax^2 + bx + c \equiv 0(mod\, p)$ for two specific binary quadratic forms. In this section, we will consider the same problem for quadratic forms $F_1^k(x,y) = 2kx^2 + kxy + 2k^2y^2$ and $F_2^k(x,y) = -3kx^2 - kxy + 3k^2y^2$, where k is an integer such that $1 \leq k \leq 10$. Here we choice these forms be able to use the results we obtained in the previous chapter. Because, the cubic congruences corresponding to these forms are

$$\begin{aligned} C_1^k &: x^3 + 2kx^2 + kx + 2k^2 \equiv 0(mod\, p) \Leftrightarrow (x^2 + k)(x + 2k) \equiv 0(mod\, p) \\ C_2^k &: x^3 - 3kx^2 - kx + 3k^2 \equiv 0(mod\, p) \Leftrightarrow (x^2 - k)(x - 3k) \equiv 0(mod\, p), \end{aligned} \quad (3)$$

respectively, that is, we come face to face with the quadratic congruences $x^2 \equiv -k$ $(mod\ p)$ and $x^2 \equiv k(mod\, p)$, respectively. For C_1^k, we set $\#C_1^k(\mathbf{F}_p) = \{x \in \mathbf{F}_p : x^3 + 2kx^2 + kx + 2k^2 \equiv 0(mod\, p)\}$. Then we have the following theorem.

Theorem 3.1. *For the cubic congruence C_1^k, we have*

$$\#C_1^1(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1(mod\, 4) \\ 1 & if\ p \equiv 3(mod\, 4) \\ 2 & if\ p = 5 \end{cases}$$

$$\#C_1^2(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,3(mod\, 8) \\ 1 & if\ p \equiv 5,7(mod\, 8) \end{cases}$$

$$\#C_1^3(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,7(mod\, 12) \\ 1 & if\ p \equiv 5,11(mod\, 12) \\ 2 & if\ p = 13 \end{cases}$$

$$\#C_1^4(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,5(mod\, 12) \\ 1 & if\ p \equiv 7,11(mod\, 4) \\ 2 & if\ p = 17 \end{cases}$$

$$\#C_1^5(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,3,7,9(mod\, 20) \\ 1 & if\ p \equiv 11,13,17,19(mod\, 20) \\ 2 & if\ p = 7 \end{cases}$$

$$\#C_1^6(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,5,7,11,25,29,31,35(mod\, 48) \\ 1 & if\ p \equiv 13,17,19,23,37,41,43,47(mod\, 48) \\ 2 & if\ p = 5 \end{cases}$$

$$\#C_1^7(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,9,11,15,23,25(mod\,28) \\ 1 & if\ p \equiv 3,5,13,17,19,27(mod\,28) \\ 2 & if\ p = 29 \end{cases}$$

$$\#C_1^8(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,11,17,19,25,35,41,43(mod\,48) \\ 1 & if\ p \equiv 5,7,13,23,29,31,37,47(mod\,48) \\ 2 & if\ p = 11 \end{cases}$$

$$\#C_1^9(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,5,13,17(mod\,24) \\ 1 & if\ p \equiv 7,11,19,23(mod\,24) \\ 2 & if\ p = 37 \end{cases}$$

$$\#C_1^{10}(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,7,9,11,13,19,23,37(mod\,40) \\ 1 & if\ p \equiv 3,17,21,27,29,31,33,39(mod\,40) \\ 2 & if\ p = 41. \end{cases}$$

Proof. For the cubic congruence C_1^k, we have

$$x^3 + 2kx^2 + kx + 2k^2 \equiv 0(mod\,p) \Leftrightarrow (x^2 + k)(x + 2k) \equiv 0(mod\,p).$$

If $k = 1$, then $C_1^1 : (x^2 + 1)(x + 2) \equiv 0(mod\,p)$. Hence $x = p - 2$ is a solution of C_1^1. If $p \equiv 1(mod\,4)$, then we know from Theorem 2.2 that the quadratic congruence $x^2 + 1 \equiv 0(mod\,p)$ has two solutions since $-1 \in Q_p$. Hence there are three solutions of C_1^1. If $p \equiv 3(mod\,4)$, then the quadratic congruence $x^2 + 1 \equiv 0(mod\,p)$ has no solution since $-1 \notin Q_p$. Hence there are one solution of C_1^1. If $p = 5$, then $C_1^1 : (x^2+1)(x+2) \equiv 0(mod\,5)$. Hence we have $x = 2, 3$ from $x^2+1 \equiv 0(mod\,5)$ and $x = 3$ from $x + 2 \equiv 0(mod\,5)$. Therefore there are two solutions $x = 2, 3$ of C_1^1 over $\mathbf{F}_5$.

Let $k = 2$. Then $C_1^2 : (x^2 + 2)(x + 4) \equiv 0(mod\,p)$. Hence $x = p - 4$ is a solution of C_1^2. If $p \equiv 1, 3(mod\,8)$, then $x^2 + 2 \equiv 0(mod\,p)$ has two solutions since $-2 \in Q_p$. Hence there are three solutions of C_1^2. If $p \equiv 5, 7(mod\,8)$, then $x^2 + 2 \equiv 0(mod\,p)$ has no solution since $-2 \notin Q_p$. Hence there are one solution of C_1^2.

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

Let $k = 3$ and $p = 13$. Then $C_1^3 : (x^2 + 3)(x + 6) \equiv 0(mod\,13)$. Hence we get $x = 6, 7$ from $x^2 + 3 \equiv 0(mod\,13)$ and $x = 7$ from $x + 6 \equiv 0(mod\,13)$. Therefore there are two integer solutions $x = 6, 7$ of C_1^3 over $\mathbf{F}_{13}$, that is, $\#C_1^3(\mathbf{F}_{13}) = 2$.

Let $k = 4$ and $p = 17$. Then $C_1^4 : (x^2 + 4)(x + 8) \equiv 0(mod\,17)$. Hence we get $x = 8, 9$ from $x^2 + 4 \equiv 0(mod\,17)$ and $x = 9$ from $x + 8 \equiv 0(mod\,17)$. Therefore there are two integer solutions $x = 8, 9$ of C_1^4 over $\mathbf{F}_{17}$.

Let $k = 5$ and $p = 7$. Then $C_1^5 : (x^2 + 5)(x + 10) \equiv 0(mod\,7)$. Hence we get $x = 3, 4$ from $x^2 + 5 \equiv 0(mod\,7)$ and $x = 4$ from $x + 10 \equiv 0(mod\,7)$. Therefore there are two integer solutions $x = 3, 4$ of C_1^5 over $\mathbf{F}_7$.

Let $k = 6$ and $p = 5$. Then $C_1^6 : (x^2 + 6)(x + 12) \equiv 0(mod\,5)$. Hence we get $x = 2, 3$ from $x^2 + 6 \equiv 0(mod\,5)$ and $x = 3$ from $x + 12 \equiv 0(mod\,5)$. Therefore there are two integer solutions $x = 2, 3$ of C_1^6 over $\mathbf{F}_5$.

Let $k = 7$ and $p = 29$. Then $C_1^7 : (x^2 + 7)(x + 14) \equiv 0(mod\,29)$. Hence we get $x = 14, 15$ from $x^2 + 7 \equiv 0(mod\,29)$ and $x = 15$ from $x + 14 \equiv 0((mod\,29)$. Therefore there are two integer solutions $x = 14, 15$ of C_1^7 over $\mathbf{F}_{29}$.

Let $k = 8$ and $p = 11$. Then $C_1^8 : (x^2 + 8)(x + 16) \equiv 0(mod\,11)$. Hence we get $x = 5, 6$ from $x^2 + 8 \equiv 0(mod\,11)$ and $x = 6$ from $x + 16 \equiv 0(mod\,11)$. Therefore there are two integer solutions $x = 5, 6$ of C_1^8 over $\mathbf{F}_{11}$.

Let $k = 9$ and $p = 37$. Then $C_1^9 : (x^2 + 9)(x + 18) \equiv 0(mod\,37)$. Hence we get $x = 18, 19$ from $x^2 + 9 \equiv 0(mod\,37)$ and $x = 19$ from $x + 18 \equiv 0(mod\,37)$. Therefore there are two integer solutions $x = 18, 19$ of C_1^9 over $\mathbf{F}_{37}$.

Finally let $k = 10$ and $p = 41$. Then $C_1^{10} : (x^2 + 10)(x + 20) \equiv 0(mod\,41)$. Hence we get $x = 20, 21$ from $x^2 + 10 \equiv 0(mod\,41)$ and $x = 21$ from $x + 20 \equiv 0(mod\,41)$. Therefore there are two integer solutions $x = 20, 21$ of C_1^{10} over $\mathbf{F}_{41}$.

For C_2^k, we set $\#C_2^k(\mathbf{F}_p) = \left\{x \in \mathbf{F}_p : x^3 - 3kx^2 - kx + 3k^2 \equiv 0(mod\,p)\right\}$. Then we have the following theorem.

Theorem 3.2. For the cubic congruence C_2^k, we have

$$\begin{aligned}
\#C_2^1(\mathbf{F}_p) &= 3 \; for\ every\ prime\ p \\
\#C_2^2(\mathbf{F}_p) &= \begin{cases} 3 & if\ p \equiv 1, 7(mod\,8) \\ 1 & if\ p \equiv 3, 5(mod\,8) \\ 2 & if\ p = 17 \end{cases} \\
\#C_2^3(\mathbf{F}_p) &= \begin{cases} 3 & if\ p \equiv 1, 11(mod\,12) \\ 1 & if\ p \equiv 5, 7(mod\,12) \\ 2 & if\ p = 13 \end{cases} \\
\#C_2^4(\mathbf{F}_p) &= \begin{cases} 2 & if\ p = 5, 7 \\ 3 & otherwise \end{cases} \\
\#C_2^5(\mathbf{F}_p) &= \begin{cases} 3 & if\ p \equiv 1, 9(mod\,10) \\ 1 & if\ p \equiv 3, 7(mod\,10) \\ 2 & if\ p = 11 \end{cases} \\
\#C_2^6(\mathbf{F}_p) &= \begin{cases} 3 & if\ p \equiv 1, 5, 19, 23(mod\,24) \\ 1 & if\ p \equiv 7, 11, 13, 17(mod\,24) \\ 2 & if\ p = 53 \end{cases} \\
\#C_2^7(\mathbf{F}_p) &= \begin{cases} 3 & if\ p \equiv 1, 3, 9, 19, 25, 27(mod\,28) \\ 1 & if\ p \equiv 5, 11, 13, 15, 17, 23(mod\,28) \\ 2 & if\ p = 31 \end{cases}
\end{aligned}$$

$$\#C_2^8(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,7,17,23(mod\, 24) \\ 1 & if\ p \equiv 5,11,13,19(mod\, 24) \\ 2 & if\ p = 71 \end{cases}$$

$$\#C_2^9(\mathbf{F}_p) = \begin{cases} 2 & if\ p = 5 \\ 3 & otherwise \end{cases}$$

$$\#C_2^{10}(\mathbf{F}_p) = \begin{cases} 3 & if\ p \equiv 1,3,9,13,27,31,37,39(mod\, 40) \\ 1 & if\ p \equiv 7,11,17,19,21,23,29,33,37(mod\, 40) \\ 2 & if\ p = 89. \end{cases}$$

Proof. For the cubic congruence C_2^k, we have

$$x^3 - 3kx^2 - kx + 3k^2 \equiv 0(mod\, p) \Leftrightarrow (x^2 - k)(x - 3k) \equiv 0(mod\, p).$$

If $k = 1$, then $C_2^1 : (x^2 - 1)(x - 3) \equiv 0(mod\, p)$. Hence $x = 3$ is a solution of C_2^1. Further the congruence $x^2 \equiv 1(mod\, p)$ has always two solutions by Theorem 2.1. Therefore there are three integer solutions of C_2^1 over $\mathbf{F}_p$ for every prime p.

Let $k = 2$. Then $C_2^2 : (x^2 - 2)(x - 6) \equiv 0(mod\, p)$. Hence $x = 6$ is a solution of C_2^2. Further by Theorem 2.1, the congruence $x^2 \equiv 2(mod\, p)$ has two solutions if $p \equiv 1,7(mod\, 8)$, and has no solution if $p \equiv 3,5(mod\, 8)$. Therefore the cubic congruence $C_2^2 : x^3 - 6x^2 - 2x + 12 \equiv 0(mod\, p)$ has three solutions if $p \equiv 1,7(mod\, 8)$ and has one solution if $p \equiv 3,5(mod\, 8)$. Now let $p = 17$. Then the cubic congruence $C_2^2 : (x^2 - 2)(x - 6) \equiv 0(mod\, 17)$ has two solutions $x = 6, 11$ since $6^2 \equiv 2(mod\, 17)$, $11^2 \equiv 2(mod\, 17)$ and also $6 \equiv 6(mod\, 17)$. The others can be proved in the same way that $\#C_2^1(\mathbf{F}_p)$ and $\#C_2^2(\mathbf{F}_p)$ were proved.

4. 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 considered this problem. In fact, this problem intimately connected to reciprocity laws. 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

$$F(x, y) = ax^2 + bxy + cy^2 = n. \tag{4}$$

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 [9] 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 $F * G$ should represent $n.m.$ The implementation of this idea is subtle and extremely difficult to describe [7]. 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 we can rewrite (4) as

$$F(x,y)=\frac{1}{a}\left(ax+\frac{b+\sqrt{\Delta}}{2}y\right)\left(ax+\frac{b-\sqrt{\Delta}}{2}y\right)=n. \tag{5}$$

Therefore we have thus expressed the problem of representation of integers by binary quadratic forms in terms of domain $R=\left\{\frac{u+v\sqrt{\Delta}}{2}: u,v\in \mathbf{Z},\ u\equiv v(mod\, 2)\right\}$. So if we take $\alpha=a$ and $\beta=\frac{b+\sqrt{\Delta}}{2}$, then (5) becomes

$$F(x,y)=\frac{1}{a}(\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y)=\frac{1}{a}N(\alpha x+\beta y), \tag{6}$$

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

In this chapter, we shall deal with the representation of prime numbers by quadratic forms F_1^k and F_2^k for $1\leq k\leq 10$.

Theorem 4.1. *For the quadratic form F_1^k, we have*

1. *Every prime number $p\equiv 5,17,23(mod\, 30)$ can be represented by F_1^1.*
2. *There is no prime number can be represented by $F_1^2, F_1^3, F_1^4, F_1^5, F_1^6, F_1^7$, F_1^8, F_1^9 and F_1^{10}.*

Proof. 1. Let $p\equiv 5,17,23(mod\, 30)$ be a prime number. The principal binary quadratic form of discriminant -15 is the form $F(x,y)=x^2+xy+4y^2$. Further the class number of forms with discriminant -15 is 2. If we check that $F(x,y)=x^2+xy+4y^2$ represents the square classes, then we see that p can be represented by $F_1^1(x,y)=2x^2+xy+2y^2$.

2. Note that F_1^k is primitive (since there is a factor k) for $k \geq 2$. So there is no prime p can be represented by F_1^k.

Now we consider F_2^k. Then we can give the following theorem without giving its proof since it can be proved in the same way that Theorem 4.1 was proved.

Theorem 4.2. *For the quadratic form F_2^k, we have*

1. *Every prime number $p \equiv 1, 3, 7, 9, 11, 25, 27, 33, 37, 41, 47, 49, 53, 63, 65, 67, 71, 73 (mod\, 74)$ can be represented by F_2^1.*
2. *There is no prime number can be represented by $F_2^2, F_2^3, F_2^4, F_2^5, F_2^6,\ F_2^7, F_2^8, F_2^9$ and F_2^{10}.*

References

[1] N. Bourbaki, *Elements of Mathematics, Commutative Algebra,* Translated from the French. Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972.

[2] J. Buchmann and U. Vollmer, *Binary Quadratic Forms: An Algorithmic Approach,* Springer-Verlag, Berlin, Heidelberg, 2007.

[3] J. Buchmann, *A generalization of Voronoi's unit algorithm I,II,* J. Number Theory **20**(1985), 177–191, 192–209.

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

[5] B.N. Delone and K. Faddeev, *The Theory of Irrationalities of the Third Degree,* Translations of Mathematical Monographs, Vol. 10 American Mathematical Society, Providence, R.I., 1964.

[6] R. Dietmann, *Small Solutions of Additive Cubic Congruences,* Arch. Math. **75** (3)(2000), 195–197.

[7] H.M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory,* Graduate Texts in Mathematics, 50. Springer-Verlag, New York-Berlin, 1977.

[8] D.E. Flath, *Introduction to Number Theory,* A Wiley-Interscience Publication. John Wiley& Sons, Inc., New York, 1989.

[9] C.F. Gauss, *Disquisitiones Arithmeticae,* English translation by Arthur A. Clarke, Yale University Press, 1966.

[10] Y.I. Manin, *On Cubic Congruences to a Prime Modulus,* Amer. Math. Soc. Transl. **13**(2)(1960).

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

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

[13] B.K. Spearman and K. Williams, *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.

[14] A. Tekcan, *The Cubic Congruence* $x^3 + ax^2 + bx + c \equiv 0(modp)$ *and Binary Quadratic Forms* $F(x, y) = ax^2\ +bxy + cy^2$*,* Ars Combinatoria **85**(2007), 257–269.

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

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

Ahmet Tekcan
Uludag University
Faculty of Science
Department of Mathematics
Görükle, Bursa-TURKIYE
email: *tekcan@uludag.edu.tr*