International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:2, No:7, 2008

# The Number of Rational Points on Elliptic Curves and Circles over Finite Fields

Betül Gezer, Ahmet Tekcan, and Osman Bizim

***Abstract*****—**In elliptic curve theory, number of rational points on elliptic curves and determination of these points is a fairly important problem. Let $p$ be a prime and $\mathbf{F}_p$ be a finite field and $k \in \mathbf{F}_p$. It is well known that which points the curve $y^2 = x^3 + kx$ has and the number of rational points of on $\mathbf{F}_p$. Consider the circle family $x^2 + y^2 = r^2$. It can be interesting to determine common points of these two curve families and to find the number of these common points. In this work we study this problem.

***Keywords*****—**Elliptic curves over finite fields, rational points on elliptic curves and circles.

## I. Introduction

Mordell began his famous paper [4] with the words "Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational points on elliptic curves". The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem in [16].

Let $p$ be a positive integer, $\mathbf{F}_p$ be a finite field, $\mathbf{F}_p^* = \mathbf{F}_p \backslash \{0\}$ and $\overline{\mathbf{F}}_p$ denote the algebraic closure of $\mathbf{F}_p$ with char($\overline{\mathbf{F}}_p$) $\neq 2, 3$. An elliptic curve $E$ over $\mathbf{F}_p$ is defined by an equation in the Weierstrass form

$$E : y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in \mathbf{F}_p$ and $4a^3 + 27b^2 \neq 0$. The discriminant and $j-$invariant of $E$ are defined by

$$\Delta = -16(4a^3 + 27b^2)$$

and

$$j = \frac{-1728(4a)^3}{\Delta},$$

respectively. We can view an elliptic curve $E$ as a curve in projective plane $\mathbf{P}^2$, with a homogeneous equation $y^2z = x^3 + axz^2 + bz^3$, together with a point at infinity. This point $\infty$ is the point where all vertical lines meet. We denote this point by $O$. The set of rational points $(x, y)$ on $E$ together with the point $O$

$$E(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = x^3 + ax + b\} \cup \{O\} \tag{2}$$

is a subgroup of $E$ (for the arithmetic of elliptic curves and rational points on them see [5], [6], [7]). The order of $E(\mathbf{F}_p)$, denoted by $\#E(\mathbf{F}_p)$, is defined as the number of points on $E$, and is given by

$$\begin{aligned} \#E(\mathbf{F}_p) &= 1 + \sum_{x \in \mathbf{F}_p} \left( \left( \frac{x^3 + ax + b}{\mathbf{F}_p} \right) + 1 \right) \\ &= p + 1 + \sum_{x \in \mathbf{F}_p} \left( \frac{x^3 + ax + b}{\mathbf{F}_p} \right), \end{aligned} \tag{3}$$

where $(\frac{\cdot}{\mathbf{F}_p})$ denotes the Legendre symbol.

Let $p > 3$ be a prime and let $k \in \mathbf{F}_p^*$ be a fixed number. In this case, in [6] and [15], the number of rational points on elliptic curves

$$E_k : y^2 = x^3 + kx \tag{4}$$

over $\mathbf{F}_p$ is given by the following:

1. If $p \equiv 3(mod\, 4)$, then $\#E(\mathbf{F}_p) = p + 1$.

2. If $p \equiv 1(mod\, 4)$, write $p = a^2+b^2$, where $a, b$ are integers with $b$ is even and $a+b \equiv 1(mod\, 4)$, then $\#E(\mathbf{F}_p) = p+1-2a$ if $k$ is a 4-th power mod $p$, $\#E(\mathbf{F}_p) = p + 1 + 2a$ if $k$ is a square mod $p$ but not a 4-th power mod $p$ and $\#E(\mathbf{F}_p) = p + 1 \pm 2b$ if $k$ is not a square mod $p$.

In [3] and [13], we consider the number of rational points on elliptic curves $y^2 = x^3 + b^2$ and $y^2 = x^3 - t^2x$ over $\mathbf{F}_p$, respectively. In this paper, we consider the intersection points of the elliptic curves

$$E_k : y^2 = x^3 + kx$$

and the circles

$$C_{r^2} : x^2 + y^2 = r^2$$

over $\mathbf{F}_p$. It is not difficult to guess that each elliptic curve may not intersect with every circle in the set of rational points. So, we will take $k = p - r^2$ and in this case, we will determine which elliptic curves and circles have common rational points and what these points are, the number of them and the number of curves and circles which have common rational points. By equating elliptic curve equation $y^2 = x^3 + kx$ with the circle equation $x^2 + y^2 = r^2$, we have the cubic equation

$$x^3 + x^2 + kx - r^2 = 0.$$

Solving this cubic equation over $\mathbf{F}_p$ is the basis of this work.

Betül Gezer, Ahmet Tekcan and Osman Bizim are with the Uludag University, Department of Mathematics, Faculty of Science, Bursa, Turkey (e-mails: betulgezer@uludag.edu.tr, tekcan@uludag.edu.tr, obizim@uludag.edu.tr).This work was supported by The Scientific and Technological Research Council of Turkey. Project no: 107T311.

## II. The Number of Rational Points on Elliptic Curves $y^2 = x^3 + kx$ and Circles $x^2 + y^2 = r^2$ Over $\mathbf{F}_p$.

Let $p > 3$ be a prime number and let

$$f(x) = x^3 + a_1x^2 + a_2x + a_3,$$

where $a_1, a_2, a_3 \in \mathbf{F}_p$. Denote the number of solutions of the congruence

$$f(x) \equiv 0(mod\ p)$$

by $N_p(f(x))$. Let

$$\begin{aligned} P &= -2a_1^3 + 9a_1a_2 - 27a_3 \\ Q &= (a_1^2 - 3a_2)^3 \\ D &= -\frac{P^2 - 4Q}{27}, \end{aligned}$$

where $D$ denotes the discriminant of the cubic polynomial $x^3+a_1x^2+a_2x+a_3$. According to Tignol [14], [10], Sun [11], [12], Dickson [2] and Skolem [8], [9], we have the following theorem.

*Theorem 2.1:* If $p > 3$ is a prime, $a_1, a_2, a_3 \in \mathbf{F}_p$ and $p$ is not divide $D$, then

$$N_p(f(x)) = \begin{cases} 0 \ \ or \ \ 3 & if \ \ (\frac{D}{p}) = 1 \\ 1 & if \ \ (\frac{D}{p}) = -1 \\ 0 & if \ \ (\frac{D}{p}) = 0. \end{cases}$$

For the cubic congruence,

$$x^3 + x^2 + kx - r^2 \equiv 0(mod\ p) \qquad (5)$$

we have

$$D = -4k^3 + k^2 - 18kr^2 - 27r^4 + 4r^2.$$

If we take $k$ and $r$ such that $k = p - r^2$, then the discriminant of the cubic congruence becomes

$$D = -4k(k + 1)^2 - p(36k + 27p + 4).$$

In this case we have,

$$D \equiv -4k(k + 1)^2(mod\ p).$$

Now we will consider two cases, either $p \equiv 1(mod\ 4)$ or $p \equiv 3(mod\ 4)$. Let $Q_p$ denote the set of quadratic residues modulo $p$.

**Case 1.** Let $p \equiv 1(mod 4)$. Since $-1 \in Q_p$ and $k \equiv -r^2(mod\ p)$, we have $k \in Q_p$. Therefore $-4k \in Q_p$ and hence $(\frac{D}{p}) = 1$. By Theorem 2.1, we know that the cubic congruence (5) has no solution or three solutions.

**Case 2.** Let $p \equiv 3(mod\ 4)$. Since $-1 \notin Q_p$, $k \in \mathbf{F}_p^*\backslash Q_p$ and $k \equiv -r^2(mod\ p)$, we have $-4k \in Q_p$. Therefore $D \equiv -4k(k + 1)^2 \in Q_p$, that is, $(\frac{D}{p}) = 1$. So also in this case, the cubic congruence (5) has no solutions or three solutions. Hence we have the following corollary:

*Corollary 2.2:* For $p > 3$ is a prime, the cubic congruence

$$x^3 + x^2 + kx - r^2 \equiv 0(mod\ p)$$

has no solution or three solutions.

Now we will show that this cubic congruence has three solutions.

*Lemma 2.1:* Let $k+r^2 = p$. Then the solutions of the cubic congruence

$$x^3 + x^2 + kx - r^2 \equiv 0(mod\ p)$$

are $r$, $-r$ and $p - 1$.

*Proof:* If we take $k = p - r^2$, then by (5) we have

$$\begin{aligned} x^3 + x^2 - r^2x - r^2 &= (x + 1)(x + r)(x - r) \\ &\equiv 0(mod\ p). \end{aligned}$$

This shows that only solutions of this congruence are $r$, $-r$ and $p - 1$. ■

Consequently, the cubic congruence $x^3 + x^2 + kx - r^2 \equiv 0(mod\ p)$ has three solutions for $k + r^2 = p$. But the points from this cubic congruence can not be the expected ones, that is, the points can not be on both elliptic curve and the circle family. Solutions of this congruence also verify the circle equation $x^2+y^2 = r^2$. In this way, for each $x$, $r^2-x^2$ must be a square in $\mathbf{F}_p$. In other words, only the solutions which make $r^2 - x^2$ a square will give us what we require. For $x = \pm r$, $r^2-x^2$ equals to zero, so it is clear that both $(r, 0)$ and $(-r, 0)$ points must be on the two curve families.

If $r^2 - (p - 1)^2$ is not a square in $\mathbf{F}_p$, then $x = p - 1$ can not be a point on both curve families. Now, we will determine that when this point is a common point of two curve families. To do this we have to consider two cases:

**Case 1.** Let $p \equiv 1(mod\ 4)$. If we write $x = p - 1$ in $y^2 = x^3 + kx$, then we have

$$y^2 = (p - 1)^3 + k(p - 1) \equiv -(k + 1)(mod\ p).$$

Since

$$-(k + 1) \in Q_p \Leftrightarrow (k + 1) \in Q_p$$

this implies that, $(p - 1, \pm\sqrt{r^2 - 1})$ are desired points if and only if $k, k + 1 \in Q_p$. We know that $k \in Q_p$. Hence

i) If $k + 1 \notin Q_p$, then common points of elliptic curve and circle family are $(r, 0)$, $(-r, 0)$.

ii) If $k + 1 \in Q_p$, then common points of elliptic curve and circle family are $(r, 0)$,$(-r, 0)$, $(p - 1, \pm\sqrt{r^2 - 1})$.

**Case 2.** Let $p \equiv 3(mod\ 4)$. In this case we know that $k \in \mathbf{F}_p^*\backslash Q_p$. Therefore

$$-(k + 1) \in Q_p \Leftrightarrow (k + 1) \in \mathbf{F}_p^*\backslash Q_p.$$

This implies that, $(p-1, \pm\sqrt{r^2-1})$ are desired points if and only if $k, k+1 \in \mathbf{F}_p^*\backslash Q_p$. We know that $k \in \mathbf{F}_p^*\backslash Q_p$. Hence

i) If $k+1 \notin \mathbf{F}_p^*\backslash Q_p$, then common points of elliptic curve and circle family are $(r, 0)$ and $(-r, 0)$.

ii) If $k+1 \in \mathbf{F}_p^*\backslash Q_p$, then common points of elliptic curve and circle family are $(r, 0)$, $(-r, 0)$, $(p-1, \pm\sqrt{r^2-1})$.

So we proved the following theorem.

*Theorem 2.3:* Let $p > 3$ be a prime and let $k + r^2 = p$. Then for elliptic curve family

$$E_k : y^2 = x^3 + kx$$

and circle family

$$C_{r^2} : x^2 + y^2 = r^2$$

with each $x$ is a solution of the equation (5), and

$$|E_k \cap C_{r^2}| = \begin{cases} 2 \quad if \ \left(\frac{r^2-x^2}{\mathbf{F}_p}\right) = 0 \\ \\ 4 \quad if \ \left(\frac{r^2-x^2}{\mathbf{F}_p}\right) = 1, \end{cases}$$

where $|E_k \cap C_{r^2}|$ denotes the number of the common points.

By generalizing the Legendre symbol to any field, $\left(\frac{r^2-x^2}{\mathbf{F}_p}\right)$ means that, $\left(\frac{r^2-x^2}{\mathbf{F}_p}\right) = 1$ if $t^2 = r^2 - x^2$ has a solution $t \in \mathbf{F}_p^*$; $\left(\frac{r^2-x^2}{\mathbf{F}_p}\right) = -1$ if $t^2 = r^2 - x^2$ has no solution $t \in \mathbf{F}_p^*$ and $\left(\frac{r^2-x^2}{\mathbf{F}_p}\right) = 0$ if $r^2 = x^2$. Thus, common points of elliptic curve and circle family are $(r, 0)$, $(-r, 0)$ and in addition to this points, we have $(p-1, \pm\sqrt{r^2-1})$ if $\left(\frac{r^2-(p-1)^2}{\mathbf{F}_p}\right) = 1$.

In $\mathbf{F}_p$, elliptic curve family $y^2 = x^3 + kx$ and circle family $x^2 + y^2 = r^2$ may not have common points. Let's see the following example.

*Example 2.1:* **1)** Let $E_2$ be the elliptic curve $y^2 = x^3 + 2x$ and $C_1$ be the circle $x^2 + y^2 = 1$ over $\mathbf{F}_7$. Then the cubic congruence

$$x^3 + x^2 + 2x - 1 \equiv 0 (mod\ 7)$$

has no solution. Therefore $E_2$ and $C_1$ have no common points in $\mathbf{F}_7$.

**2)** Let $E_4$ be the elliptic curve $y^2 = x^3 + 4x$ and $C_2$ be the circle $x^2 + y^2 = 2$ over $\mathbf{F}_7$. Then the cubic congruence

$$x^3 + x^2 + 4x - 2 \equiv 0 (mod\ 7)$$

has only one solution $x \equiv 5(mod\ 7)$. Then from the circle equation we yield, $4 + y^2 \equiv 2(mod\ 7)$ or $y^2 \equiv 5(mod\ 7)$, but $5 \notin Q_7$. So there is no $y$ value, satisfying this equation. Therefore $E_4$ and $C_2$ have no common points in $\mathbf{F}_7$.

Now we will determine how many circles and elliptic curves have intersection for a prime $p$. We have to consider following two cases.

**Case 1.** Let $p \equiv 1(mod\ 4)$. Then $k \in Q_p$ and $k + r^2 = p$. So elliptic curve and circle family have intersection. Thus, the number of intersection of these two curve families is $|Q_p|$, namely there are

$$\frac{p-1}{2}$$

circles and elliptic curves families which have intersection.

**Case 2.** Let $p \equiv 3(mod\ 4)$. Then $k \in \mathbf{F}_p^*\backslash Q_p$. So there are

$$p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$$

circles and elliptic curves families which have intersection, that is, in this case the number of intersection of these two curve families is $\frac{p-1}{2}$, too.

*Corollary 2.4:* For a prime $p > 3$, the number of intersection of the elliptic curve family $y^2 = x^3 + kx$ and the circle family $x^2 + y^2 = r^2$ in $\mathbf{F}_p$ is

$$\frac{p-1}{2}.$$

*Example 2.2:* Let $E_k : y^2 = x^3 + kx$ and $C_{r^2} : x^2 + y^2 = r^2$.

**1)** If $p = 13$, then we have the following table:

| $k$ | $r^2$ | $points$ |
|---|---|---|
| 1 | 12 | $(5,0), (8,0)$ |
| 3 | 10 | $(6,0), (7,0), (12,3), (12,10)$ |
| 4 | 9 | $(3,0), (10,0)$ |
| 9 | 4 | $(2,0), (11,0), (12,4), (12,9)$ |
| 10 | 3 | $(4,0), (9,0)$ |
| 12 | 1 | $(1,0), (12,0)$ |

**2)** If $p = 19$, then we have the following table:

| $k$ | $r^2$ | $points$ |
|---|---|---|
| 2 | 17 | $(6,0), (13,0), (18,4), (18,15)$ |
| 3 | 16 | $(4,0), (15,0)$ |
| 8 | 11 | $(7,0), (12,0)$ |
| 10 | 9 | $(3,0), (16,0)$ |
| 12 | 7 | $(11,0), (8,0), (18,5), (18,14)$ |
| 13 | 6 | $(5,0), (14,0), (18,9), (18,10)$ |
| 14 | 5 | $(9,0), (10,0), (18,2), (18,17)$ |
| 15 | 4 | $(2,0), (17,0)$ |
| 18 | 1 | $(1,0), (18,0)$ |

Now we will determine the number of intersection of elliptic curve and circle families which has the points $(r,0)$, $(-r,0)$ and $(r,0)$, $(-r,0)$, $(p-1,\pm\sqrt{r^2-1})$. We have to consider two cases as we did before. But we need to know the following theorem. In [1] it is given that,

*Theorem 2.5:* Let $N(p)$ denote the number of pairs of consecutive quadratic residues modulo $p$ in $\mathbf{F}_p$. Then

$$N(p)=\frac{(p-4-(-1)^{\frac{p-1}{2}})}{4}.$$

Let $N(p)^*$ denote the number of pairs of consecutive integers in $\mathbf{F}_p$, where the first is a quadratic nonresidue and the second is a quadratic nonresidue modulo $p$ and

$$N(p)^*=\frac{(p-2+(-1)^{\frac{p-1}{2}})}{4}.$$

Then we have two cases:

**Case 1.** Let $p\equiv 1(mod\ 4)$. Then $(p-1,\pm\sqrt{r^2-1})$ are desired points if and only if $k,k+1\in Q_p$ by the proof of Theorem 2.3. Hence, by Theorem 2.5, the number of cases where the intersection of elliptic curve and circle has four points which are $(p-1,\pm\sqrt{r^2-1})$ and $(\pm r,0)$ is

$$N(p)=\frac{(p-4-(-1)^{\frac{p-1}{2}})}{4}$$

and the number of cases where the intersection of elliptic curve and circle has two points which are $(\pm r,0)$ is

$$\frac{p-1}{2}-N(p)=\frac{p-(-1)^{\frac{p-1}{2}}}{4}=\frac{p+2+(-1)^{\frac{p-1}{2}}}{4}.$$

*Example 2.3:* Let $p=13$. Then the number of cases where the intersection of elliptic curve and circle has four points which are $(p-1,\pm\sqrt{r^2-1})$ and $(\pm r,0)$ is

$$N(13)=\frac{(13-4-(-1)^{\frac{13-1}{2}})}{4}=2$$

and the number of cases where the intersection of elliptic curve and circle has two points which are $(\pm r,0)$ is

$$\frac{13-1}{2}-N(13)=6-2=4.$$

These curves can be seen in Example 2.2.

**Case 2.** Let $p\equiv 3(mod\ 4)$. Then $(p-1,\pm\sqrt{r^2-1})$ are desired points if and only if $k,k+1\in\mathbf{F}_p^*\backslash Q_p$ by the proof of Theorem 2.3. Hence by Theorem 2.5, the number of cases where the intersection of elliptic curve and circle has four points which are $(p-1,\pm\sqrt{r^2-1})$ and $(\pm r,0)$ is

$$N(p)^*=\frac{(p-2+(-1)^{\frac{p-1}{2}})}{4}$$

and the number of cases where the intersection of elliptic curve and circle has two points which are $(\pm r,0)$ is

$$\begin{aligned}\frac{p-1}{2}-N(p)^* &= \frac{p-1}{2}-\frac{(p-2+(-1)^{\frac{p-1}{2}})}{4}\\ &= \frac{p-(-1)^{\frac{p-1}{2}}}{4}.\end{aligned}$$

*Example 2.4:* Let $p=19$. Then the number of cases where the intersection of elliptic curve and circle has four points which are $(p-1,\pm\sqrt{r^2-1})$ and $(\pm r,0)$ is

$$N(19)^*=\frac{(19-2+(-1)^{\frac{19-1}{2}})}{4}=4$$

and the number of cases where the intersection of elliptic curve and circle has two points which are $(\pm r,0)$ is

$$\frac{19-1}{2}-N(19)^*=9-4=5.$$

These curves can be seen in Example 2.2.

Therefore we have the following result.

*Theorem 2.6:* The number of cases where the intersection of elliptic curve and circle has four points which are $(p-1,\pm\sqrt{r^2-1})$ and $(\pm r,0)$ is

$$\begin{cases} N(p)=\frac{(p-4-(-1)^{\frac{p-1}{2}})}{4} & if\ p\equiv 1(mod\ 4)\\ N(p)^*=\frac{(p-2+(-1)^{\frac{p-1}{2}})}{4} & if\ p\equiv 3(mod\ 4)\end{cases}$$

and the number of cases where the intersection of elliptic curve and circle has two points which are $(\pm r,0)$ is

$$\begin{cases} \frac{p-1}{2}-N(p)=\frac{p+2+(-1)^{\frac{p-1}{2}}}{4} & if\ p\equiv 1(mod\ 4)\\ \frac{p-1}{2}-N(p)^*=\frac{p-(-1)^{\frac{p-1}{2}}}{4} & if\ p\equiv 3(mod\ 4).\end{cases}$$

We can also determine how many points are there in the intersection of the elliptic curve $y^2=x^3+kx$ and circle $x^2+y^2=r^2$. We know that there are the points $(\pm r,0)$, and we know that there are $\frac{p-1}{2}$ elliptic curve families. So the number of these points is

$$2\left(\frac{p-1}{2}\right)=p-1.$$

In addition to these points, there are the points $(p-1,\pm\sqrt{r^2-1})$. So if $p\equiv 1(mod\ 4)$, then the number of these points is

$$2N(p)$$

and if $p\equiv 3(mod\ 4)$ then the number of these points is

$$2N(p)^*.$$

Therefore we have the following corollary.

*Corollary 2.7:* The number of the common points of the elliptic curve family $y^2=x^3+kx$ together with the circle family $x^2+y^2=r^2$ is

$$\begin{cases} p-1+2N(p)=\frac{3p-6-(-1)^{\frac{p-1}{2}}}{2} & if\ p\equiv 1(mod\ 4)\\ p-1+2N(p)^*=\frac{3p-4+(-1)^{\frac{p-1}{2}}}{2} & if\ p\equiv 3(mod\ 4).\end{cases}$$

*Example 2.5:* **1)** Let $p = 13$. Then the number of the common points of the elliptic curve family together with the circle family is

$$13 - 1 + 2N(13) = 16.$$

**2)** Let $p = 19$. Then the number of the common points of the elliptic curve family together with the circle family is

$$19 - 1 + 2N(19)^{*} = 26.$$

For any numbers $k$ and $r$ if $(\frac{D}{p}) = 1$, then the cubic congruence (5) has either no solution or three solutions. If the cubic congruence (5) has no solution, then elliptic curve family and circle family have any common points. Let the cubic congruence (5) has three solutions. In this case, if for each three solution $x$, and $r^2 - x^2$ is a square in $\mathbf{F}_p$, then elliptic curve and circle have six common points. If for two solutions $r^2 - x^2$ is a square in $\mathbf{F}_p$, then they have four common points and if for one solution $r^2 - x^2$ is a square in $\mathbf{F}_p$, then they have two common points. Furthermore, if $\left(\frac{r^2-x^2}{\mathbf{F}_p}\right) = 0$ namely, $r^2 - x^2 = 0$, then there are two or four common points, as we seen before in our case. Therefore, in the general case they may have zero, two, four or six common points.

*Example 2.6:* **1)** Let $E_1 : y^2 = x^3 + x$ and $C_4 : x^2 + y^2 = 4$ over $\mathbf{F}_{13}$. Then the cubic congruence

$$x^3 + x^2 + x - 4 \equiv 0(mod\ 13)$$

has no solution. Therefore $E_1$ and $C_4$ have no common points.

**2)** Let $E_6 : y^2 = x^3 + 6x$ and $C_9 : x^2 + y^2 = 9$ over $\mathbf{F}_{19}$. Then the cubic congruence

$$x^3 + x^2 + 6x - 9 \equiv 0(mod\ 19)$$

has three solutions which are $x_1 = 4$, $x_2 = 5$ and $x_3 = 9$. It can be seen that only one solution makes $r^2 - x^2$ a square in $\mathbf{F}_{19}$. In fact, for $x_1 = 4$ we get that $16 + y^2 \equiv 9(mod\ 19)$ or $y^2 \equiv 12(mod\ 19)$, but $12 \notin Q_{19}$. So there is no $y$ value satisfying this equation and we have no points. For $x_2 = 5$ we get that $6 + y^2 \equiv 9(mod\ 19)$ or $y^2 \equiv 3(mod\ 19)$, but $3 \notin Q_{19}$. So there is no $y$ value satisfying this equation and we have no points and for $x_3 = 9$ from the circle equation we get that $5 + y^2 \equiv 9(mod\ 19)$ or $y^2 \equiv 4(mod\ 19)$. So we have the points $(9, 2)$, $(9, 17)$. Therefore elliptic curve $E_6$ and circle $C_9$ have two common points.

**3)** Let $E_1 : y^2 = x^3 + x$ and $C_1 : x^2 + y^2 = 1$ over $\mathbf{F}_{11}$. Then the cubic congruence

$$x^3 + x^2 + x - 1 \equiv 0(mod\ 11)$$

has three solutions which are $x_1 = 5, x_{2,3} = 8$. It also can be easily seen that these solutions make $r^2 - x^2$ a square in $\mathbf{F}_{11}$. In fact, for $x_1 = 5$ from the circle equation we get that $3 + y^2 \equiv 1(mod\ 11)$ or $y^2 \equiv 9(mod\ 11)$. So we have the points $(5, 5)$, $(5, 12)$ and for $x_{2,3} = 8$ we get that $9 + y^2 \equiv 1(mod\ 11)$ or $y^2 \equiv 3(mod\ 11)$. So we have the points $(8, 5)$, $(8, 6)$. Therefore elliptic curve $E_1$ and circle $C_1$ have four common points.

**4)** Let $E_{14} : y^2 = x^3 + 14x$ and $C_{16} : x^2 + y^2 = 16$ over $\mathbf{F}_{17}$. Then the cubic congruence

$$x^3 + x^2 + 14x - 16 \equiv 0(mod\ 17)$$

has three solutions which are $x_1 = 1$, $x_2 = 5$ and $x_3 = 10$. It can be easily seen that these solutions make $r^2 - x^2$ a square in $\mathbf{F}_{17}$. In fact, for $x_1 = 1$ from the circle equation we get that $1 + y^2 \equiv 16(mod\ 17)$ or $y^2 \equiv 15(mod\ 17)$. So we have the points $(1, 7)$, $(1, 10)$ and for $x_2 = 5$ we get that $8 + y^2 \equiv 16(mod\ 17)$ or $y^2 \equiv 8(mod\ 17)$. So we have the points $(5, 5)$, $(5, 12)$ and for $x_3 = 10$ we get that $15 + y^2 \equiv 16(mod\ 17)$ or $y^2 \equiv 1(mod\ 17)$. So we have the points $(10, 1)$ and $(10, 16)$. Therefore elliptic curve $E_{14}$ and circle $C_{16}$ have six common points.

In second case, for any numbers $k$ and $r$ if $(\frac{D}{p}) = -1$, then the cubic congruence (5) has only one solution $x$ and if for this solution, $r^2 - x^2$ is a square in $\mathbf{F}_p$, then the elliptic curve and circle have two common points over $\mathbf{F}_p$. Therefore in this case, they may have zero or two common points.

Let's see these situations in the following example.

*Example 2.7:* **1)** If $E_1 : y^2 = x^3 + x$ and $C_1 : x^2 + y^2 = 1$ over $\mathbf{F}_7$. Then the cubic congruence

$$x^3 + x^2 + x - 1 \equiv 0(mod\ 7)$$

has only one solution which is $x = 5$. We can easily see that this solution makes $r^2 - x^2$ a square in $\mathbf{F}_7$. In fact, for $x = 5$ from the circle equation we get that $4 + y^2 \equiv 1(mod\ 7)$ or $y^2 \equiv 4(mod\ 7)$. So we have the points $(5, 2)$ and $(5, 5)$. Therefore $E_1$ and $C_1$ have two common points.

**2)** If $E_3 : y^2 = x^3 + 3x$ and $C_1 : x^2 + y^2 = 1$ over $\mathbf{F}_7$. Then the cubic congruence

$$x^3 + x^2 + 3x - 1 \equiv 0(mod\ 7)$$

has only one solution which is $x = 4$. We can easily see that this solution does not make $r^2 - x^2$ a square in $\mathbf{F}_7$. In fact, for $x = 4$ from the circle equation we get that $2 + y^2 \equiv 1(mod\ 7)$ or $y^2 \equiv 6(mod\ 7)$, but $6 \notin Q_7$. So there is no $y$ value satisfying this equation and so we have no points. Therefore elliptic curve $E_3$ and circle $C_1$ have no common points.

## References

[1] G.E. Andrews. *Number Theory.* Dover Pub., 1971.

[2] L.E. Dickson. *Criteria for irreducibility of functions in a finite field.* Bull, Amer. Math. Soc. **13**(1906), 1–8.

[3] B. Gezer, H. Özden, A. Tekcan and O. Bizim. *The Number of Rational Points on Elliptic Curves $y^2 = x^3 + b^2$ over Finite Fields.* IInternational Journal of Mathematics Sciences **1**(3)(2007), 178–184.

[4] L.J. Mordell. *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees.* Proc. Cambridge Philos. Soc. **21**(1922), 179–192.

[5] R. Schoof. *Counting Points on Elliptic Curves Over Finite Fields.* Journal de Theorie des Nombres de Bordeaux, **7**(1995), 219–254.

[6] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[7] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer, 1992.

[8] T. Skolem. *Zwei Sätze über kubische Kongruenzen.* Norske Vid. Selsk. Forhdl. **10**(1937) 89–92.

[9] T. Skolem. *On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod $p$.* Norsk Math. Tidsskr. **34**(1952) 81–85.

[10] L. Stickelberger. *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper.* Verhand. I, Internat. Math. Kongress Zürich, 1897, pp. 182–193.

[11] Z.H. Sun. *Cubic and quartic congruences modulo a prime.* Journal of Number Theory **102**(2003), 41–89.

[12] Z.H. Sun. *Cubic residues and binary quadratic forms.* Journal of Number Theory, to be printed.

[13] A. Tekcan. *The Elliptic Curves $y^2 = x^3 - t^2x$ over $\mathbf{F}_p$.* International Journal of Mathematics Sciences **1**(3)(2007), 165–171.

[14] J.P. Tignol. *Galois Theory of Algebraic Equations.* World Scientific Publishing Co., Singapore, New Jersey, 2001, pp. 38–107.

[15] L.C. Washington. *Elliptic Curves, Number Theory and Cryptography.* Chapman&Hall/CRC, Boca London, New York, Washington DC, 2003.

[16] A. Wiles. *Modular Elliptic Curves and Fermat's Last Theorem.* Ann. of Math. **141**(3)(1995), 443–551.