

# Rational Points on Elliptic Curves $y^2 = x^3 + a^3$ in $\mathbf{F}_p$ , where $p \equiv 5 \pmod{6}$ is Prime

Gokhan Soydan, Musa Demirci, Nazli Yildiz İkikardes, Ismail Naci Cangul

**Abstract**—In this work, we consider the rational points on elliptic curves over finite fields  $\mathbf{F}_p$  where  $p \equiv 5 \pmod{6}$ . We obtain results on the number of points on an elliptic curve  $y^2 \equiv x^3 + a^3 \pmod{p}$ , where  $p \equiv 5 \pmod{6}$  is prime. We give some results concerning the sum of the abscissae of these points. A similar case where  $p \equiv 1 \pmod{6}$  is considered in [5]. The main difference between two cases is that when  $p \equiv 5 \pmod{6}$ , all elements of  $\mathbf{F}_p$  are cubic residues.

**Keywords**—Elliptic curves over finite fields, rational points

## I. INTRODUCTION

Let  $\mathbf{F}$  be a field of characteristic not equal to 2 or 3. An elliptic curve  $E$  defined over  $\mathbf{F}$  is given by an equation

$$y^2 = x^3 + Ax + B \in \mathbf{F}[x] \quad (1)$$

where  $A, B \in \mathbf{F}$  so that  $4A^3 + 27B^2 \neq 0$  in  $\mathbf{F}$ . The set of all solutions  $(x, y) \in \mathbf{F} \times \mathbf{F}$  to this equation together with a point  $\circ$ , called the point at infinity, is denoted by  $E(\mathbf{F})$ , called the set of  $\mathbf{F}$ -rational points on  $E$ . The value  $\Delta(E) = -16(4A^3 + 27B^2)$  is called the discriminant of elliptic curve  $E$ . For a more detailed information about elliptic curves in general, see [4].

For any two points  $P(x_1, y_1)$  and  $Q(x_2, y_2)$  on  $E$ , define

$$P + Q = \begin{cases} \circ & \text{if } x_1 = x_2 \text{ and } y_1 + y_2 = 0, \\ Q & \text{if } P = \circ \\ (x_3, y_3) & \text{otherwise} \end{cases}$$

where

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

and

$$m = \begin{cases} (y_2 - y_1) / (x_2 - x_1) & \text{if } P \neq Q \\ (3x_1^2 + A) / 2y_1 & \text{if } P = Q \end{cases}$$

where  $y_1 \neq 0$ , while when  $y_1 = 0$ , the point is of order 2. With this definition,  $E(\mathbf{F})$  forms an additive abelian group having identity  $\circ$ . Here, by definition,  $-P = (x, -y)$  for a point  $P = (x, y)$  on  $E$ .

It has always been interesting to look for the number of points over a given field  $\mathbf{F}$ . In [3], three algorithms to find

Gokhan Soydan, Musa Demirci, Ismail Naci Cangul are with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, emails: gsoydan@uludag.edu.tr, mdemirci@uludag.edu.tr, cangul@uludag.edu.tr. Nazli Yildiz İkikardes is with the Balıkesir University, Department of Mathematics, Faculty of Science, Balıkesir-TURKEY. email: nyildiz@balikesir.edu.tr. This work was supported by the research fund of Uludag University project no: F-2003/63.

the number of points on an elliptic curve over a finite field. Among the well-known results, there are the followings:

**Theorem 1.1:** (Mordell,1922) Let  $E$  be an elliptic curve given by an equation

$$E : y^2 = x^3 + Ax + B$$

with  $A, B \in \mathbf{Q}$ . There is a finite set of points  $P_1, P_2, \dots, P_r$  so that every point  $P$  in  $E(\mathbf{Q})$  can be obtained as a sum

$$P = n_1.P_1 + n_2.P_2 + \dots + n_r.P_r$$

with  $n_1, n_2, \dots, n_r \in \mathbf{Z}$ . In other words,  $E(\mathbf{Q})$  is a finitely generated group.

**Theorem 1.2:** (Mazur,1977) The group  $E(\mathbf{Q})$  contains at most 16 points of finite order.

If, in particular, we take  $A, B \in \mathbf{Z}$  and look for the integer solutions of (1), we have

**Theorem 1.3:** (Siegel,1928) An elliptic curve

$$E : y^2 = x^3 + Ax + B \in \mathbf{Z}[x]$$

with  $A, B \in \mathbf{Z}$  and  $\Delta \neq 0$  has only finitely many points  $P(x, y)$  with integer coordinates.

## II. THE GROUP $E(\mathbf{F}_p)$ OF POINTS MODULO

$$p, p \equiv 5 \pmod{6}$$

It is interesting to solve polynomial congruences modulo  $p$ . Clearly, it is much easier to find solutions in  $\mathbf{F}_p$  for small  $p$ , than to find them in  $\mathbf{Q}$ . Because, in  $\mathbf{F}_p$ , there is always a finite number of solutions.

In this work, we consider the elliptic curve (1) in modulo  $p$ , for  $A = 0$  and  $B = a^3$ , where  $a$  is an integer, and try to obtain results concerning the number of points on  $E$  over  $\mathbf{F}_p$  and also their orders.

In [10], starting with a conjecture from 1952 of Dénes which is a variant of Fermat-Wiles theorem, Merel illustrates the way in which Frey elliptic curves have been used by Taylor, Ribet, Wiles and the others in the proof of Fermat-Wiles theorem. Serre, in [11], gave a lower bound for the Galois representations on elliptic curves over the field  $\mathbf{Q}$  of rational points. In the case of a Frey curve, the conductor  $N$  of the curve is given by the help of the constants in the  $abc$  conjecture. In [9], Ono recalls a result of Euler, known as Euler's concordant forms problem, about the classification of those pairs of distinct non-zero integers  $M$  and  $N$  for which there are integer solutions  $(x, y, t, z)$  with  $xy \neq 0$  to  $x^2 + My^2 = t^2$  and  $x^2 + Ny^2 = z^2$ . When  $M = -N$ , this becomes the congruent number problem, and when  $M = 2N$ , by replacing  $x$  by  $x - N$  in  $E(2N, N)$ , a special form of

the Frey elliptic curves is obtained as  $y^2 = x^3 - N^2x$ . Using Tunnell's conditional solution to the congruent number problem using elliptic curves and modular forms, Ono studied the elliptic curve  $y^2 = x^3 + (M + N)x^2 + MNx$  denoted by  $E_Q(M, N)$  over  $Q$ . He classified all the cases and hence reduced Euler's problem to a question of ranks. In [7], Parshin obtains an inequality to give an effective bound for the height of rational points on a curve. In [8], the problem of boundedness of torsion for elliptic curves over quadratic fields is settled.

If  $F$  is a field, then an elliptic curve over  $F$  has, after a change of variables, a form

$$y^2 = x^3 + Ax + B$$

where  $A$  and  $B \in F$  with  $4A^3 + 27B^2 \neq 0$  in  $F$ . Here  $D = -16(4A^3 + 27B^2)$  is called the discriminant of the curve. Elliptic curves are studied over finite and infinite fields. Here we take  $F$  to be a finite prime field  $F_p$  with characteristic  $p > 3$ . Then  $A, B \in F_p$  and the set of points  $(x, y) \in F_p \times F_p$ , together with a point  $o$  at infinity is called the set of  $F_p$ -rational points of  $E$  on  $F_p$  and is denoted by  $E(F_p)$ .  $N_p$  denotes the number of rational points on this curve. It must be finite.

In fact one expects to have at most  $2p + 1$  points (together with  $o$ ) (for every  $x$ , there exist a maximum of 2  $y$ 's). But not all elements of  $F_p$  have square roots. In fact only half of the elements of  $F_p$  have a square root. Therefore the expected number is about  $p + 1$ .

Here we shall deal with Bachet elliptic curves  $y^2 = x^3 + a^3$  modulo  $p$ . Some results on these curves have been given in [5], and [6].

A historical problem leading to Bachet elliptic curves is that how one can write an integer as a difference of a square and a cube. In another words, for a given fixed integer  $c$ , search for the solutions of the Diophantine equation  $y^2 - x^3 = c$ . This equation is widely called as Bachet or Mordell equation. This is because L. J. Mordell, in twentieth century, made a lot of advances regarding this and some other similar equations. The existence of duplication formula makes this curve interesting. This formula was found in 1621 by Bachet. When  $(x, y)$  is a solution to this equation where  $x, y \in Q$ , it is easy to show that  $(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3})$  is also a solution for the same equation. Furthermore, if  $(x, y)$  is a solution such that  $xy \neq 0$  and  $c \neq 1, -432$ , then this leads to infinitely many solutions, which could not proven by Bachet. Hence if an integer can be stated as the difference of a cube and a square, this could be done in infinitely many ways. For example if we start by a solution  $(3, 5)$  to  $y^2 - x^3 = -2$ , by applying duplication formula, we get a series of rational solutions  $(3, 5), (\frac{129}{10^2}, \frac{-383}{10^3}), (\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}), \dots$

It can easily be seen that an elliptic curve

$$y^2 = x^3 + a^3 \tag{2}$$

can have at most  $2p + 1$  points in  $\mathbf{Z}_p$ ; i.e. the point at infinity along with  $2p$  pairs  $(x, y)$  with  $x, y \in F_p$ , satisfying the equation (2). This is because, for each  $x \in F_p$ , there are at most two possible values of  $y \in F_p$ , satisfying (2).

But not all elements of  $F_p$  has a square root. In fact, only half of the elements in  $F_p^* = F_p \setminus \{0\}$  have square roots. Therefore the expected number of points on  $E(F_p)$  is about  $p + 1$ .

It is known, as a more precise formula, that the number of solutions to (2) is

$$p + 1 + \sum \chi(x^3 + a^3)$$

where  $\chi(a) = (\frac{a}{p})$  denotes the Legendre symbol which is equal to  $+1$  if  $a$  is a quadratic residue modulo  $p$ ;  $-1$  if not; and  $0$  if  $p|a$ , ([4], pp132). The following theorem of Hasse quantifies this result:

*Theorem 2.1:* (Hasse,1922) An elliptic curve (2) has

$$p + 1 + \delta$$

solutions  $(x, y)$  modulo  $p$ , where  $|\delta| < 2\sqrt{p}$ .

Equivalently, the number of solutions is bounded above by the number  $(\sqrt{p} + 1)^2$ .

From now on, we will only consider the case  $p$  is prime congruent to 5 modulo 6. The other possible case where  $p \equiv 1 \pmod{6}$  has been discussed in [5]. We begin by some calculations regarding the number of points on (2). First we have the following particular case. But we first need the following lemma:

*Lemma 2.1:* Let  $p$  be a prime. If  $(p - 1, 3) = d = 1$ , then the congruence  $x^3 \equiv a \pmod{p}$  has a solution for each  $a \in F_p$ , that is every  $a \in F_p$  is a cubic residue.

*Proof:* When  $(p - 1, 3) = 1$ , we have either  $p = 3$  or  $p \equiv 2 \pmod{3}$ , as  $p$  is prime. If  $p = 3$ , then  $0^3 \equiv 0 \pmod{3}$ ,  $1^3 \equiv 1 \pmod{3}$  and  $2^3 \equiv 2 \pmod{3}$  in  $F_3$  and therefore every  $a \in F_3$  is a cubic residue. Secondly, if  $p \equiv 2 \pmod{3}$  is prime, then  $p = 2 + 3k$  for  $k \in \mathbf{Z}$ . Therefore the norm of  $p$  is

$$N_p = p.p = (2 + 3k).(2 + 3k) = 9k^2 + 12k + 4$$

and

$$\frac{N_p - 1}{3} = 3k^2 + 4k + 1.$$

Now for  $a \in F_p^*$ , we have

$$a^{\frac{(N_p - 1)}{3}} = a^{3k^2 + 4k + 1}$$

By Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod{p}.$$

Then

$$a^{p-1} \equiv a^{3k+2-1} \equiv a^{3k+1} \equiv 1 \pmod{p}.$$

Therefore

$$a^{\frac{(N_p - 1)}{3}} \equiv (a^{3k+1})^{k+1} \equiv 1^{k+1} \equiv 1 \pmod{p}.$$

Let's now choose an element  $a$  between 1 and  $p-1$  and choose an integer  $k$  between 0 and  $p-2$ . Let  $g$  be a primitive root modulo  $p$  such that

$$g^k \equiv a \pmod{p}.$$

Since  $(3, p - 1) = 1$ , there are integers  $x'$  and  $y'$  such that

$$3x' + (p - 1).y' = 1.$$

Then by putting  $x = x'k$  and  $y = y'k$ , this equation becomes

$$3x + (p - 1).y = k$$

Now, as  $g^{p-1} \equiv 1 \pmod{p}$ , we have

$$a \equiv g^k \equiv g^{3x+(p-1).y} \equiv (g^x)^3(g^{p-1})^y \equiv (g^x)^3 \pmod{p}$$

That means,  $a$  is a cubic residue modulo  $p$ . Further as  $0^3 \equiv 0 \pmod{p}$ , all elements of  $\mathbf{F}_p$  are cubic residues. ■

**Theorem 2.2:** Let  $p \equiv 5 \pmod{6}$  be prime. Then there are exactly  $p + 1$  rational points on the curve

$$y^2 \equiv x^3 + a^3 \pmod{p}.$$

*Proof:* By Lemma 5, all elements of  $\mathbf{F}_p$  are cubic residues modulo  $p$ ,  $p \equiv 5 \pmod{6}$ . For every quadratic residue  $q$  in  $\mathbf{F}_p$ , there are two solutions  $y_1 = t$  and  $y_2 = p - t$  of  $y^2 \equiv q \pmod{p}$ . It is well known, see [1], that the number of such  $q$  is equal to the order of  $Q_p$ , the group of quadratic residues modulo  $p$ , which is equivalent to  $\frac{p-1}{2}$ . Then we must look for  $x \in \mathbf{F}_p$  such that  $x^3 + a^3 \equiv q \pmod{p}$ . Hence  $x^3 \equiv q - a^3 \pmod{p}$  and since  $q - a^3 \in \mathbf{F}_p$ , there is only one solution of  $x^3 \equiv q - a^3 \pmod{p}$  in  $\mathbf{F}_p$ . That is, for each of  $\frac{p-1}{2}$  quadratic residues, there is exactly one solution of the congruence  $x^3 \equiv q - a^3 \pmod{p}$  since  $(p-1, 3) = 1$ . That means that there is a total of  $\frac{p-1}{2}$  values of  $x$ . Going backwards, we find  $2.\frac{p-1}{2} = p - 1$  rational points, since there exist two different values of  $y$  for each  $x$ . By adding the obvious point  $(-a, 0)$  and the point at infinity, the result follows. ■

**Corollary 2.3:** Let  $p \equiv 5 \pmod{6}$  be prime. Then there are either no values or 2 values of  $y \in \mathbf{F}_p$  for every  $x \in \mathbf{F}_p - \{a\}$  such that  $(x, y)$  lies on the curve  $y^2 \equiv x^3 + a^3 \pmod{p}$ . When this number is 2, the sum of these values of  $y$  is equal to  $p$ . Further for  $x = a$ , there is only one point  $(a, 0)$  on the curve.

*Proof:* Follows by Theorem 6. ■

**Corollary 2.4:** Among all rational points on the curve

$$y^2 \equiv x^3 + a^3 \pmod{p},$$

the sum of ordinates of the points with the same abscissa is either 0 or  $p$ .

**Corollary 2.5:** Let  $p \equiv 5 \pmod{6}$  be prime. Then the number of all possible different values of  $x$  obtained for  $y = 0, 1, 2, \dots, p - 1$  in the equation

$$y^2 \equiv x^3 + a^3 \pmod{p},$$

is  $\frac{p+1}{2}$ .

*Proof:* Follows by Corollary 8 as  $1 + \frac{p-1}{2} = \frac{p+1}{2}$ . ■

In Theorem 6, we have seen that the curve  $y^2 \equiv x^3 + a^3 \pmod{p}$  has exactly  $p + 1$  rational points. We further can say that no two of these points have the same ordinate:

**Theorem 2.6:** Let  $p \equiv 5 \pmod{6}$  be prime. Then no two points on the curve

$$y^2 \equiv x^3 + a^3 \pmod{p}$$

have the same ordinate.

*Proof:* Let  $u \equiv y^2 - a^3 \pmod{p}$ . As each element of  $\mathbf{F}_p$  is a cubic residue,  $u$  is a cubic residue. Then the congruence  $x^3 \equiv u \pmod{p}$  has solutions, and the number of these solutions can not be more than 3, as  $p$  is prime. By Theorem 6,

it is known that there are exactly  $p$  rational points  $(x, y)$  apart from the point at infinity on  $y^2 \equiv x^3 + a^3 \pmod{p}$ . Since there are  $p$  values of modulo  $p$ , for each such value,  $x^3 \equiv u \pmod{p}$  can have only one solution. ■

**Theorem 2.7:** Let  $p \equiv 5 \pmod{6}$  be prime. There are exactly

$$1 + \sum_{x \in \mathbf{F}_p} \rho(x)$$

values of  $x$  such that there are two values of  $y$ , having a sum equal to  $p$ , where the rational point  $(x, y)$  is on the curve  $y^2 \equiv x^3 + a^3 \pmod{p}$ . This number is therefore equivalent to  $\frac{p+1}{2}$ . Here

$$\rho(x) = \begin{cases} 2 & \text{if } \chi(x^3 + a^3) = 1 \\ 0 & \text{if } \chi(x^3 + a^3) = -1 \\ 1 & \text{if } \chi(x^3 + a^3) = 0 \end{cases}$$

*Proof:* For  $x = 0, 1, 2, \dots, p - 1$  calculate the values  $x^3 + a^3 \pmod{p}$ . If  $x^3 + a^3 \in Q_p$ , i.e. if  $\chi(x^3 + a^3) = 1$ , then there are exactly two values of  $y \in U_p$ , such that  $y^2 \equiv x^3 + a^3 \pmod{p}$ . By Theorem 6, there are exactly  $p + 1$  points on the curve with integer coefficients. Apart from the point at infinity and the point  $(-a, 0)$ , the others have ordinates different than 0. Since they are paired so that the ordinates of each pair add up to  $p$ , the number of all possible values of  $x$  is  $\frac{p+1}{2}$ . ■

Note that the number given in this theorem is three less than the number given for  $p \equiv 1 \pmod{6}$  in [5]. This is because the cubic root  $w = \frac{-1 + \sqrt{3}i}{2}$  is not in  $\mathbf{F}_p$  in this case.

We can easily formulate the sum of abscissae of all points on the curve  $y^2 \equiv x^3 + a^3 \pmod{p}$ .

**Theorem 2.8:** Let  $p \equiv 5 \pmod{6}$  be prime. The sum of abscissae of the points on the curve  $y^2 = x^3 + a^3 \pmod{p}$  having integer coefficients is equal to

$$\sum_{x \in \mathbf{F}_p} (1 + \chi_p(x^3 + a^3)).x$$

*Proof:* It is clear from the definition of the function  $\chi_p$ .

**Theorem 2.9:** Let  $p \equiv 5 \pmod{6}$  be prime. Then there is a unique  $\mathbf{F}_p$ -point on the curve

$$y^2 \equiv x^3 + a^3 \pmod{p}$$

with  $y \equiv 0 \pmod{p}$ , which is  $(-a, 0)$ .

*Proof:* Let  $y \equiv 0 \pmod{p}$ . Then  $x^3 \equiv a^3 \pmod{p}$ , and hence

$$(x - a)(x^2 + ax + a^2) \equiv 0 \pmod{p}$$

iff

$$x \equiv a \pmod{p} \text{ or } x^2 + ax + a^2 \equiv 0 \pmod{p}.$$

Now,  $x \equiv a \pmod{p}$  is obvious solution. To have another solution, one must be able to solve

$$(x + b)^2 \equiv -3b^2 \pmod{p}.$$

To do this,  $-3$  must be a quadratic residue modulo  $p$ . i.e.  $\left(\frac{-3}{p}\right) = +1$  must be satisfied. But it is well-known that  $\left(\frac{-3}{p}\right) = -1$  for  $p \equiv 2 \pmod{3}$  is prime, see, e.g. ([2], pp 93 - 94). ■

**Conclusion 2.1:** One can generalize the result concerning the number of  $\mathbf{F}_p$ -points on an elliptic curve using the Weil conjecture as explained below:

*Theorem 2.10:* (Weil Conjecture) The Zeta-function is a rational function of  $T$  having the form

$$Z(T; E/\mathbf{F}_q) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}$$

where only the integer  $a$  depends on the particular elliptic curve  $E$ . The value  $a$  is related to  $N = N_1$  as follows:

$$N = q + 1 - a.$$

In addition, the discriminant of the quadratic polynomial in the numerator is negative, and so the quadratic has two conjugate roots  $\frac{1}{\alpha}$  and  $\frac{1}{\beta}$  with absolute value  $\frac{1}{\sqrt{q}}$ . Writing the numerator in the form  $(1 - \alpha T)(1 - \beta T)$  and taking the derivatives of logarithm both sides, one can obtain the number of  $F_{q^r}$ - points on  $E$ , denoted by  $N_r$ , as follows:

$$N_r = q^r + 1 - \alpha^r - \beta^r, r = 1, 2, \dots$$

*Example 2.1:* Let us find the  $\mathbf{F}_{25}$ -points on the elliptic curve  $y^2 = x^3 + 8$ . There are  $N_1 = 6$   $\mathbf{F}_5$ -points on the elliptic curve:

$$(1, 2), (1, 3), (2, 1), (2, 4), (3, 0)$$

and  $\circ$ . Now as  $r = 2$  we want to find

$$N_2 = 25 + 1 - \alpha^2 - \beta^2.$$

To find the "reciprocal roots"  $\alpha$  and  $\beta$ , we first consider the formula

$$N_1 = q + 1 - a.$$

Hence

$$6 = 5 + 1 - a$$

gives  $a = 0$ . Then we consider the quadratic equation

$$1 + 5T^2 = 0,$$

which has two roots  $\frac{\pm i}{\sqrt{5}}$ . Then  $\alpha = \sqrt{5}i$  and  $\beta = -\sqrt{5}i$  and finally

$$N_r = \begin{cases} 5^r + 1 & \text{if } r \text{ is odd} \\ 5^r + 1 - 2 \cdot (-5)^{\frac{r}{2}} & \text{if } r \text{ is even} \end{cases}.$$

Hence we found

$$N_2 = 5^2 + 1 - 2(-5)^{\frac{2}{2}} = 36.$$

Similarly  $N_3 = 5^3 + 1 = 126$  and  $N_4 = 576$  can be calculated.

*Example 2.2:* Let us find the  $\mathbf{F}_{25}$ -points on the elliptic curve  $y^2 = x^3 - x$ . There are  $N_1 = 8$   $\mathbf{F}_5$ -points on the elliptic curve:

$$(0, 0), (1, 0), (2, 1), (2, 4), (3, 2), (3, 3), (4, 0)$$

and  $\circ$ . Now as  $r = 2$  we want to find

$$N_2 = 25 + 1 - \alpha^2 - \beta^2.$$

To find the "reciprocal roots"  $\alpha$  and  $\beta$ , we first consider the formula

$$N_1 = q + 1 - a.$$

Hence

$$8 = 5 + 1 - a$$

gives  $a = -2$ . Then we consider the quadratic equation

$$1 + 2T + 5T^2 = 0,$$

which has two roots  $\frac{-1 \pm 2i}{5}$ . Then  $\alpha = -1 + 2i$  and  $\beta = -1 - 2i$  and finally

$$N_2 = 26 - (-1 + 2i)^2 - (-1 - 2i)^2 = 32.$$

Similarly  $N_3 = 104$  can be calculated.

#### REFERENCES

- [1] Jones, G.A., Jones, J.M., *Elementary Number Theory*, Springer-Verlag, (1998), ISBN 3-540-76197-7
- [2] Esmonde, J. & Murty, M. R., *Problems in Algebraic Number Theory*, Springer-Verlag, (1999), ISBN 0-387-98617-0.
- [3] Schoof, R., *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux, 7(1995), 219-254.
- [4] Silverman, J.H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, (1986), ISBN 0-387-96203-4.
- [5] Demirci, M. & Soydan, G. & Cangül, I. N., *Rational points on the elliptic curves  $y^2 = x^3 + a^3 \pmod{p}$  in  $\mathbf{F}_p$  where  $p \equiv 1 \pmod{6}$  is prime*, Rocky J. of Maths, ( to be printed ).
- [6] Soydan, G. & Demirci, M. & İkikardeş, N. Y. & Cangül, I. N., *Rational points on the elliptic curves  $y^2 = x^3 + a^3 \pmod{p}$  in  $\mathbf{F}_p$  where  $p \equiv 5 \pmod{6}$  is prime*, (submitted).
- [7] Parshin, A. N., *The Bogomolov-Miyaoka-Yau inequality for the arithmetical surfaces and its applications*, Seminaire de Theorie des Nombres, Paris, 1986-87, 299-312, Progr. Math., 75, Birkhauser Boston, MA, 1998.
- [8] Kamienny, S., *Some remarks on torsion in elliptic curves*, Comm. Alg. 23 (1995), no. 6, 2167-2169.
- [9] Ono, K., *Euler's concordant forms*, Acta Arith. 78 (1996), no. 2, 101-123.
- [10] Merel, L., *Arithmetic of elliptic curves and Diophantine equations*, Les XXemes Journees Arithmetiques (Limoges, 1997), J. Theor. Nombres Bordeaux 11 (1999), no. 1, 173-200.
- [11] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259-331.