ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 37, Number 5, 2007

RATIONAL POINTS ON ELLIPTIC CURVES $y^2 = x^3 + a^3$ IN $\mathbf{F}_p$ WHERE $p \equiv 1 \pmod 6$ IS PRIME

MUSA DEMIRCI, GOKHAN SOYDAN, ISMAIL NACI CANGUL

ABSTRACT. In this work, we consider the rational points on elliptic curves over finite fields $\mathbf{F}_p$. We give results concerning the number of points on the elliptic curve $y^2 \equiv x^3 + a^3 \pmod p$ where p is a prime congruent to 1 modulo 6. Also some results are given on the sum of abscissae of these points. We give the number of solutions to $y^2 \equiv x^3 + a^3 \pmod p$, also given in [**1**, page 174], this time by means of the quadratic residue character, in a different way, by using the cubic residue character. Using the Weil conjecture, one can generalize the results concerning the number of points in $\mathbf{F}_p$ to $\mathbf{F}_{p^r}$.

1. 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

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

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 $E(\mathbf{F})$ and called the set of $\mathbf{F}$-rational points on E. The value $\Delta(E) = -16(4A^3 + 27B^2)$ is called the discriminant of the elliptic curve E. For more detailed information about elliptic curves in general, see [**4**].

The $E(\mathbf{F})$ 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 the number of points on an elliptic curve over a finite field are given.

2000 AMS *Mathematics subject classification.* Primary 11G20, 14H25, 14K15, 14G99.
Keywords and phrases. Elliptic curves over finite fields, rational points.
This work was supported by the research fund of Uludağ University project no: F-2003/63.
Received by the editors on February 15, 2005, and in revised form on April 26, 2005.