ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 24, Number 3, Summer 1994

ON THE EQUATION $Y^2 = (X + p)(X^2 + p^2)$

ROEL J. STROEKER AND JAAP TOP

ABSTRACT. In this paper the family of elliptic curves over $\mathbf{Q}$ given by the equation $y^2 = (x + p)(x^2 + p^2)$ is studied. It is shown that for p a prime number $\equiv \pm 3 \bmod 8$, the only rational solution to the equation given here is the one with $y = 0$. The same is true for $p = 2$. Standard conjectures predict that the rank of the group of rational points is odd for all other primes p. A lot of numerical evidence in support of this is given. We show that the rank is bounded by 3 in general for prime numbers p. Moreover, this bound can only be attained for certain special prime numbers $p \equiv 1 \bmod 16$. Examples of such rank 3 curves are given. Lastly, for certain primes $p \equiv 9 \bmod 16$ nontrivial elements in the Shafarevich group of the elliptic curve are constructed. In the literature one finds similar investigations of elliptic curves with complex multiplication. It may be interesting to note that the curves considered here do not admit complex multiplication.

1. Introduction. Let p be a prime number. Throughout this paper $E_p/\mathbf{Q}$ will denote the elliptic curve given by the equation $y^2 = (x+p)(x^2+p^2)$. The change of variable $x = \xi - p$ yields another model $y^2 = \xi(\xi^2 - 2p\xi + 2p^2)$ for E_p. This paper is devoted to the study of the finitely generated abelian group $E_p(\mathbf{Q})$ consisting of the $\mathbf{Q}$-rational points on E_p. The torsion subgroup of $E_p(\mathbf{Q})$ is given by

Proposition 1.1. *$E_p(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/2\mathbf{Z}$, with the $\mathbf{Q}$-rational point having $y = 0$ as a generator.*

Proof. If $l \in \mathbf{Z}$, $l \geq 5$ is a prime where E_p has good reduction (i.e., $l \neq 2$ and $l \neq p$), then the homomorphism 'reduction modulo l' : $E_p(\mathbf{Q})_{\text{tor}} \to E_p(\mathbf{F}_l)$ is known to be injective [**12**, p. 176]. Now for $l = 5, 7, 11$ and $p \neq 5, 7, 11$, respectively, $E_p(\mathbf{F}_l)$ consists of 6 ± 2, respectively 8 ± 2, respectively 12 ± 4, points; the sign depending on whether p is a square modulo l or not. From this, it follows that the torsion subgroup of $E_p(\mathbf{Q})$ has order at most 2. Since it always contains a point of order 2 the proposition follows. □

Received by the editor on July 2, 1993.