Mathematical Journal of Okayama University

Volume 49, *Issue* 1 2007 *Article* 12

JANUARY 2007

Elliptic Curves $y^2=x^3-px$ of Rank Two

Blair K. Spearman*

*University of British Columbia Okanagan

Elliptic Curves $y^2=x^3-px$ of Rank Two

Blair K. Spearman

Abstract

A class of prime numbers p is given for which the elliptic curve $y^2 = x^3 - px$ has rank two. This extends a theorem of Kudo and Motose.

KEYWORDS: Elliptic curve, rank

Math. J. Okayama Univ. **49** (2007), 183–184

ELLIPTIC CURVES $y^2 = x^3 - px$ OF RANK TWO

Blair K. SPEARMAN

Abstract. A class of prime numbers p is given for which the elliptic curve $y^2 = x^3 - px$ has rank two. This extends a theorem of Kudo and Motose.

Let p be a prime number and let E denote the elliptic curve $y^2 = x^3 - px$. We let $E(\mathbb{Q})$ be the set of rational points on E. Then $E(\mathbb{Q})$ has the structure of a finitely generated abelian group. We write

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{\text{tors}}$ is a finite group and where r is a non-negative integer called the Mordell-Weil rank of E. In [2] it was shown that $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$. Further, the authors showed that $r = 2$, the maximal rank for this type of elliptic curve, if p is a Fermat prime > 5, that is $p = 2^{2^n} + 1$ with $n \geq 2$. The purpose of this paper is to extend the class of primes for which $r = 2$. We prove the following theorem.

Theorem 1. *Let p be an odd prime number such that $p = u^4 + v^4$ for some integers u and v. Then*

$$E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}.$$

We note that Fermat primes $p > 5$ are of the form $u^4 + v^4$.

Proof. Since $u^4 + v^4 = p$ is odd, we have $(u, v) = 1$ and exactly one of u, v is odd. The calculation of the rank of $E(\mathbb{Q})$ uses the method described in [2]. For more details see [1] or [3]. Briefly, the idea for this problem is to consider E simultaneously with the curve $y^2 = x^3 + 4px$ denoted by $\bar{E}$. Begin by writing down two families of equations, one for each curve according to [1, Theorem 7.6]. For the curve E these equations are $dS^4 + cT^4 = U^2$ where $(d, c) = (p, -1)$ or $(-1, p)$. The number of these equations having integral solutions (S, T, U) with $S, T \geq 1$, and $(S, c) = 1$ is equal to $2^w - 2$ for some positive integer w. An analogous statement holds for the curve $\bar{E}$ where $2^{\bar{w}} - 2$ of the equations $dS^4 + cT^4 = U^2$ are solvable with $(d, c) = (2, 2p)$ or $(2p, 2)$ because $dS^4 + cT^4 = U^2$ has no solution for $d < 0$ and $c < 0$. Then the rank of $E(\mathbb{Q})$ is equal to $w + \bar{w} - 2$ from [1, Corollary 7.5].

Mathematics Subject Classification. 11G05.

Key words and phrases. Elliptic curve, rank.

Research was supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

The equation $pS^4 - T^4 = U^2$ has a solution $(S, T, U = (1, v, v^2)$ and clearly $(S, c) = 1$ where $p = u^4 + v^4$.

The equation $-S^4 + pT^4 = U^2$ has a solution $(S, T, U) = (v, 1, u^2)$ and $(S, c) = (v, p) = 1$ for otherwise $p \mid v$ so that $0 \equiv p = u^4 + v^4 \equiv u^4 \pmod p$ implying that $p \mid u$ contradicting $(u, v) = 1$.

We may assume $u > v$. The equation $2S^4 + 2pT^4 = U^2$ has a solution $(S, T, U) = (u - v, 1, 2u^2 - 2uv + 2v^2)$. If $u \equiv v \pmod 2$ then we have a contradiction from $p = u^4 + v^4 \equiv 2u^4 \equiv 0 \pmod 2$. If $u \equiv v \pmod p$, then $0 \equiv p = u^4 + v^4 \equiv 2u^4 \pmod p$ so we have a contradiction $0 \equiv u \equiv v \pmod p$. Thus $(S, c) = (u - v, 2p) = 1$.

Finally we consider the equation $2pS^4 + 2T^4 = U^2$ which has a solution $(S, T, U) = (1, u - v, 2u^2 - 2uv + 2v^2)$ and $(S, c) = 1$ where $p = u^4 + v^4$.

From these observations $w = \bar{w} = 2$ so the rank of $E(\mathbb{Q}) = w + \bar{w} - 2 = 2$. This completes the proof. □

Let S denote the set of primes of the form $x^4 + y^4$ and less than 10,000. Then we have

$$S = \{17, 97, 257, 337, 641, 881, 1297, 2417, 2657, 3697, 4177, 4721, 6577\}$$

References

[1] J.S. Chahal, *Topics in number theory,* Kluwer Academic/Plenum Publisher, 1988.

[2] T. Kudo and K. Motose, *On Group structures of some special elliptic curves,* Math. J. Okayama Univ. **47** (2005), 81-84.

[3] J.H. Silverman and J. Tate, *Rational points on elliptic curves,* Springer New York, 1985.

Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B.C. Canada V1V 1V7
e-mail address: blair.spearman@ubc.ca

(*Received July 6, 2006*)
(*Revised September 21, 2006*)