

On the Group Structure of Elliptic Curves $y^2 = x^3 - 2px$

Blair K. Spearman¹

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

Abstract

A condition is given on integers of the form $2p$ for p a prime so that the elliptic curve $y^2 = x^3 - 2px$ has rank three.

Mathematics Subject Classification: 11G05

Keywords: Elliptic curve, rank

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

$$\Gamma \simeq T \oplus \mathbb{Z}^r,$$

where T is a finite group (the torsion subgroup) and r is a non-negative integer called the Mordell-Weil rank of E . The purpose of this paper is to give a condition under which the rank r of the curve $y^2 = x^3 - 2px$ is equal to 3, the maximal rank for this type of curve. This condition requires that we represent $2p$ by a polynomial in two variables. We give the complete group structure for these curves. Elliptic curves of the form $y^2 = x^3 - px$ were considered in [2] and [4].

Theorem. *Let p be a prime number such that $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$ for some integers u and v . Then*

$$\Gamma \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}.$$

¹Research was supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

Proof. The calculation of the rank of Γ uses a method which is described in [3, pp. 89-94] .(see also [1]) Let \mathbb{Q}^* be the multiplicative group of non-zero rational numbers and let \mathbb{Q}^{*2} denote the subgroup of squares of elements of \mathbb{Q}^* . We make use of the group homomorphism α from Γ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ defined as follows.

$$\alpha(P) = \begin{cases} 1 \pmod{\mathbb{Q}^{*2}} & \text{for } P = O, \text{ the point at infinity,} \\ b \pmod{\mathbb{Q}^{*2}} & \text{for } P = (0, 0), \\ x \pmod{\mathbb{Q}^{*2}} & \text{for } P = (x, y) \text{ with } x \neq 0. \end{cases}$$

The group $\alpha(\Gamma)$ consists modulo \mathbb{Q}^{*2} of 1, b , and all divisors b_1 of b such that $b_1 \not\equiv 1, b \pmod{\mathbb{Q}^{*2}}$ and for which the equation $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ with $b_1b_2 = b$ has an integral solution (N, M, e) with $M \neq 0, e \neq 0$ satisfying the GCD conditions $(N, e) = (M, e) = (b_1, e) = (b_2, M) = (M, N) = 1$.

Simultaneously we study a second curve $y^2 = x(x^2 - 2ax + a^2 - 4b)$ denoted by \bar{E} with group of rational points $\bar{\Gamma}$. In an analogous manner, we introduce a second group homomorphism $\bar{\alpha}$ from $\bar{\Gamma}$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

$$\bar{\alpha}(P) = \begin{cases} 1 & \pmod{\mathbb{Q}^{*2}} & \text{for } P = O, \text{ the point at infinity,} \\ a^2 - 4b & \pmod{\mathbb{Q}^{*2}} & \text{for } P = (0, 0), \\ 1 & \pmod{\mathbb{Q}^{*2}} & \text{for } P = (x, y) \text{ with } x \neq 0. \end{cases}$$

The group $\bar{\alpha}(\bar{\Gamma})$ consists modulo \mathbb{Q}^{*2} of 1, $a^2 - 4b$, and all divisors b_1 of $a^2 - 4b$ such that $b_1 \not\equiv 1, a^2 - 4b \pmod{\mathbb{Q}^{*2}}$ and for which the equation $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ with $b_1b_2 = a^2 - 4b$ has an integral solution (N, M, e) with $M \neq 0, e \neq 0$ satisfying the GCD conditions $(N, e) = (M, e) = (b_1, e) = (b_2, M) = (M, N) = 1$.

The rank r of the given curve E satisfies

$$2^r = \frac{|\alpha(\Gamma)| |\bar{\alpha}(\bar{\Gamma})|}{4}. \tag{1}$$

To determine the order of $\alpha(\Gamma)$ (or $\bar{\alpha}(\bar{\Gamma})$) we consider only enough of the equations $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ (or $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$) so that combined with the group structure of $\alpha(\Gamma)$ (or $\bar{\alpha}(\bar{\Gamma})$) the order of these groups is completely determined.

We begin by calculating $|\alpha(\Gamma)|$. For our given elliptic curve E , we have $a = 0$ and $b = -2p$. Modulo \mathbb{Q}^{*2} , $\alpha(\Gamma)$ contains 1, $-2p$ together with a subset of $\{-1, 2, -2, p, -p, 2p\}$. We give solutions of two equations $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$. The equations and their solutions are given in the table below. The GCD conditions are checked by noting that $e = 1$ or $M = 1$ and observing that $(u, v) = 1$ and u is odd if the condition of the

theorem holds. Some of the GCD conditions can be examined efficiently by using resultants. For example when $b_1 = -1$, suppose we want to confirm that $(M, N) = 1$. Referring to the table below for the expressions for M and N , a calculation shows that the resultants of M and N with respect to u , then v are 2^8v^8 and 2^8u^8 . Any common prime divisor of M and N would divide both of these. Since $(u, v) = 1$, this common prime divisor would have to be 2. However this is impossible as u is odd so that M is odd resulting in $(M, N) = 1$.

Equations for E

$$N^2 = b_1M^4 + b_2e^4, \quad b_1b_2 = -2p, \quad 2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$$

b_1	b_2	Equation	(N, M, e)
-1	$2p$	$N^2 = -M^4 + 2pe^4$	$((u^2 - 2v^2)^2, u^2 + 2v^2, 1)$
p	-2	$N^2 = pM^4 - 2e^4$	$(u^4 - 4v^4, 1, 2uv)$

We conclude that $\alpha(\Gamma)$ contains $\{1, -2p, -1, p\}$. Modulo \mathbb{Q}^{*2} this set of 4 elements generates a group which is all of $\{1, -2p, -1, p, -p, 2p, -2, 2\}$. Therefore $|\alpha(\Gamma)| = 8$.

Next we calculate $|\bar{\alpha}(\bar{\Gamma})|$. For our elliptic curve \bar{E} we have $a^2 - 4b = 8p$. Following the same method as the first part of the proof we make use of the fact that modulo \mathbb{Q}^{*2} , $\bar{\alpha}(\bar{\Gamma})$ contains 1, $8p$ together with a subset of $\{-1, 2, -2, p, -p, -2p\}$. This time $\bar{\alpha}(\bar{\Gamma})$ cannot contain any of the negative values $-1, -2, -p, -2p$ since the equation $N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ would have a right hand side which cannot assume positive values. To determine $\bar{\alpha}(\bar{\Gamma})$ we choose $b_1 = 8$ and note that $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ becomes $N^2 = 8M^4 + pe^4$ which has the solution $(N, M, e) = (3u^4 + 4v^4, u^2, 1)$. The GCD conditions are checked in the same way as they were in the first part of this proof. Since $8 \equiv 2 \pmod{\mathbb{Q}^{*2}}$ we conclude that $\bar{\alpha}(\bar{\Gamma})$ contains $\{1, 2p, 2, p\}$, with the last element included by closure. Since this is the maximal size for $\bar{\alpha}(\bar{\Gamma})$ (all positive values of b_1) we see that $|\bar{\alpha}(\bar{\Gamma})| = 4$. Finally using (1) we conclude that the rank r satisfies

$$2^r = \frac{|\alpha(\Gamma)| |\bar{\alpha}(\bar{\Gamma})|}{4} = \frac{8 \cdot 4}{4} = 8$$

so that $r = 3$.

The calculation of the torsion subgroup T is achieved using reduction modulo primes. The discriminant for the curve $y^2 = x^3 - 2px$ equals 2^5p^3 and $p = 41$ is the smallest prime to which the hypothesis of the theorem applies. Therefore we deduce that 3 and 5 cannot divide 2^5p^3 so they are primes of

good reduction. Modulo 3, $y^2 = x^3 - 2px$ reduces to either $y^2 = x^3 - x$ or $y^2 = x^3 - 2x$, each of which has four points over the finite field \mathbb{F}_3 . Modulo 5, $y^2 = x^3 - 2px$ reduces to $y^2 = x^3 - 2x$ and it is easy to check that $y^2 = x^3 - 2x$ has ten points over \mathbb{F}_5 . Since $|T|$ divides both 4 and 10, we conclude that $|T| \leq 2$. However $(0, 0)$ is a point of order two so $T \simeq \mathbb{Z}/2\mathbb{Z}$ as required. \square

Integers less than 10^8 of the form $2p$ for some prime p , such that with $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4$ for some integers u and v are

$$\{82, 8962, 17042, 83522, 213842, 811282, 2109442, 3421202\}$$

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.
- [4] B.K. Spearman, Elliptic Curves $y^2 = x^3 - px$ of rank two. Accepted by Math. J. Okayama Univ.

Received: November 15, 2006