QUADRATIC FORMS AND ELLIPTIC CURVES III

KEN ONO# AND TAKASHI ONO

There have been many investigations regarding the distribution of ranks of elliptic curves in natural families, and it is believed that the vast majority of elliptic curves E over $\mathbb{Q}$ have rank ≤ 1. Consequently the identification of elliptic curves with rank ≥ 2 is of some interest. Most studies have dealt with families of elliptic curves over $\mathbb{Q}$ which are quadratic twists or cubic twists of a single base curve (see [2,4]). In this note we examine elliptic curves over $\mathbb{Q}$ given by the Weierstrass model

$$E(b): \quad y^2 = x^3 - (b^2 + b)x \tag{0}$$

where $b \neq 0, -1$ is an integer. These curves form a natural family in the sense that they all have have $j = 1728$ and they contain the *canonical* points

$$P_b := \big((b + 1/2)^2, (b + 1/2)(b^2 + b - 1/4)\big)$$

of infinite order which are afforded by the theory of Hopf maps. This family of curves is a special case of Theorem 3.10 [3] where many families of positive rank elliptic curves are given.

Here we show, subject to the *Parity Conjecture*, that one can construct infinitely many curves $E(b)$ with even rank ≥ 2. Briefly recall that the Parity Conjecture states that an elliptic curve E over $\mathbb{Q}$ with rank r satisfies

$$(-1)^r = \omega(E) \tag{1}$$

where $\omega(E)$ is the sign of the functional equation of the Hasse-Weil $L-$function $L(E, s)$.

First we begin with some preliminaries. Birch and Stephens (see [1]) computed the sign of the functional equation, denoted $\omega(E_D)$, for the elliptic curve

$$E_D : y^2 = x^3 - Dx.$$

If $D \not\equiv 0 \pmod 4$ is a fourth power free integer, then $\omega(E_D)$ is given by

$$\omega(E_D) := \operatorname{sgn}(-D) \cdot \epsilon(D) \cdot \prod_{p^2 || D} \left(\frac{-1}{p}\right), \tag{2}$$

The first author is supported by NSF grants DMS-9508976 and DMS-9304580.

where the product is over primes $p \geq 3$, and $\epsilon(D)$ is given by

$$\epsilon(D) := \begin{cases} -1 & \text{if } D \equiv 1, 3, 11, 13 \pmod{16}, \\ 1 & \text{if } D \equiv 2, 5, 6, 7, 9, 10, 14, 15 \pmod{16}. \end{cases} \tag{3}$$

For questions concerning rank, there is no loss in generality if we assume that $D \not\equiv 0 \pmod 4$. This follows from the fact that $y^2 = x^3 + D'x$ is 2−isogenous to $y^2 = x^3 - 4D'x$.

Returning to the curves $E(b)$, we find that $b^2 + b \equiv 0 \pmod 4$ if and only if $b \equiv 0, 3 \pmod 4$. However it is easy to see that for such b we may assume that $b \not\equiv 0 \pmod{16}$, since $b^2 + b$ would then be divisible by 16, a fourth power. Consequently if $b \equiv 0, 3 \pmod 4$ and $b^2 + b$ is fourth power free, then $\frac{b^2+b}{4}$ is not a multiple of 4. So to compute $\omega(E(b))$, we simply need to compute $\omega\left(E_{-\frac{b^2+b}{4}}\right)$ using (2) and (3). In particular we find that for such b

$$\omega(E(b)) = \epsilon\left(-\frac{b^2+b}{4}\right) \cdot \prod_{p^2 || b^2+b} \left(\frac{-1}{p}\right). \tag{4}$$

In particular if $b \equiv 0, 3 \pmod 4$ is an integer for which $b^2 + b$ is fourth power free, then

$$\omega(E(b)) = \begin{cases} \prod_{p^2||b^2+b} \left(\frac{-1}{p}\right) & \text{if } b \equiv 7, 8, 11, 12, 20, 23, 24, 28, 35, 39, 40, \\ & \qquad 43, 51, 52, 55, 56 \pmod{64} \\ -\prod_{p^2||b^2+b} \left(\frac{-1}{p}\right) & \text{if } b \equiv 3, 4, 19, 27, 36, 44, 59, 60 \pmod{64}. \end{cases} \tag{5}$$

If $b^2 + b \not\equiv 0 \pmod 4$ is a fourth power free, then $\omega(E(b)) = \omega(E_{b^2+b})$, and $\epsilon(b^2 + b) = 1$. Therefore directly by (2) and (3) we obtain

$$\omega(E(b)) = -\prod_{p^2||b^2+b} \left(\frac{-1}{p}\right). \tag{6}$$

As a consequence of the Parity Conjecture we obtain the following immediate theorem.

Theorem. *Let $b \neq 0, -1$ be an integer for which $b^2 + b$ is fourth power free, and define T by*

$$T := \text{card}\{p \mid \text{primes } \ 3 \leq p \equiv 3 \pmod 4, \ p^2 || (b^2 + b)\}.$$

Assuming the Parity Conjecture, then the following are true:

1. *If $b \equiv 1, 2 \pmod 4$ and T is odd, then $E(b)$ has even rank ≥ 2.*
2. *If $b \equiv 7, 8, 11, 12, 20, 23, 24, 28, 35, 39, 40, 43, 51, 52, 55, 56 \pmod{64}$ and T is even, then then $E(b)$ has even rank ≥ 2.*
3. *If $b \equiv 3, 4, 19, 27, 36, 44, 59, 60 \pmod{64}$ and T is odd, then $E(b)$ has even rank ≥ 2.*
4. *In all other cases, $E(b)$ has odd rank.*

By part (2) of the above Theorem we obtain the following immediate corollaries:

Corollary 1. *If $b' \equiv 2, 3, 5, 6, 7, 10, 13, 14 \pmod{16}$ and both b' and $4b' + 1$ are square-free, then assuming the Parity Conjecture $E(4b')$ has even rank ≥ 2.*

Corollary 2. *If $b \equiv 7, 11, 23, 35, 39, 43, 51, 55 \pmod{64}$ and $\frac{b^2+b}{4}$ is square-free, then assuming the Parity Conjecture $E(b)$ has even rank ≥ 2.*

In closing, we note that the only positive integers $b \leq 400$ for which $E(b)$ has even rank > 2 are $b = 156, 231, 387$. In these cases $E(b)$ has rank 4.

References

1. B. J. Birch and N.M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295-299.
2. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1-23.
3. T. Ono, *Quadratic forms and elliptic curves*, preprint.
4. C. Stewart and J. Top, *On ranks of twists of elliptic curves and power free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 947-974.

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540

E-mail address: ono@math.ias.edu

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802

E-mail address: ono@math.psu.edu

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland 21218

E-mail address: ono@chow.mat.jhu.edu