

### Quadratic Forms and Elliptic Curves. III\*)

By Ken ONO\*\*\*) and Takashi ONO\*\*\*\*)

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1996)

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  $\leq 1$ . Consequently the identification of elliptic curves with rank  $\geq 2$  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

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

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

$P_b := ((b + 1/2)^2, (b + 1/2)(b^2 + b - 1/4))$  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  $\geq 2$ . Briefly recall that the Parity Conjecture states that an elliptic curve  $E$  over  $\mathbb{Q}$  with rank  $r$  satisfies

$$(1) \quad (-1)^r = \omega(E)$$

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

$$(2) \quad \omega(E_D) := \text{sgn}(-D) \cdot \varepsilon(D) \cdot \prod_{p^2 \mid D} \left(\frac{-1}{p}\right),$$

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

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

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  $\omega(E_{-\frac{b^2+b}{4}})$  using (2) and (3). In particular

$$(4) \quad \omega(E(b)) = \varepsilon\left(-\frac{b^2 + b}{4}\right) \cdot \prod_{p^2 \mid b^2 + b} \left(\frac{-1}{p}\right).$$

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

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

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

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

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

**Theorem.** *Let  $b \neq 0$ ,  $-1$  be an integer for*

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

\*\*) School of Mathematics, Institute for Advanced Study, U.S.A.

\*\*\*\*) Department of Mathematics, The Johns Hopkins University, U.S.A.