Fudge Factors in the Birch and Swinnerton-Dyer Conjecture

Karl Rubin

The aim of this note is to describe how the "fudge factors" in the Birch and Swinnerton-Dyer conjecture vary in a family of quadratic twists (see Proposition 5, which follows directly from Tate's algorithm [T]). We illustrate with two examples.

Definition 1. If E is an elliptic curve over $\mathbf{Q}$ and p is a prime, the *fudge factor* (or *Tamagawa factor*) $c_p(E)$ is defined by

$$c_p(E) = [E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$$

where $E_0(\mathbf{Q}_p)$ is the subgroup of $E(\mathbf{Q}_p)$ consisting of those points whose reduction modulo p (on a minimal model of E) is nonsingular.

The fundamental method for computing the fudge factors is Tate's algorithm. This algorithm, originally described in a 1965 letter to Cassels, was published in [T] and essentially reproduced in §IV.9 of [S]. Standard number theoretic computer packages, such as PARI/GP (available at `http://pari.math.u-bordeaux.fr`), will compute these factors very efficiently.

Let $\Delta(E)$ denote the discriminant of a minimal model of E.

Proposition 2. Suppose E is an elliptic curve over $\mathbf{Q}$.

1. If E has good reduction at p, then $c_p(E) = 1$.
2. If E has split multiplicative reduction at p, then $c_p(E) = \mathrm{ord}_p(\Delta(E))$, i.e., $p^{c_p(E)}$ is the highest power of p dividing $\Delta(E)$.
3. If E has nonsplit multiplicative reduction at p, then $c_p(E) \le 2$ and $c_p(E) \equiv \mathrm{ord}_p(\Delta(E)) \pmod 2$.
4. If E has additive reduction at p, then $c_p(E) \le 4$.

Proof. These are cases 1, 2a, 2b, and 3 through 10, respectively, of Tate's algorithm [T]. □

[0]Supported by NSF grant DMS-0140378.

Fix an elliptic curve E and a model of E of the form

$$y^2 = f(x)$$

with a monic cubic polynomial $f(x) \in \mathbf{Z}[x]$, and let Δ denote the discriminant of this model. We may assume that the model is minimal at all primes $p > 2$, but this is not necessary for what follows.

Definition 3. The quadratic twist of E by a nonzero rational number d is

$$E_d : y^2 = d^3 f(x/d).$$

We will write simply $c_p(d)$ for $c_p(E_d)$. The purpose of this note is to describe how $c_p(d)$, and $\prod_p c_p(d)$, vary with d.

Lemma 4. Suppose $d, d' \in \mathbf{Q}^\times$.

1. If d/d' is a square in $\mathbf{Q}$, then E_d is isomorphic to $E_{d'}$.
2. If p is a prime and d/d' is a square in $\mathbf{Q}_p$, then $c_p(d) = c_p(d')$.

Proof. If $d' = dr^2$, then the map $(x, y) \mapsto (r^2 x, r^3 y)$ is an isomorphism from E_d to $E_{d'}$. If $r \in \mathbf{Q}^\times$, this proves (i). If $r \in \mathbf{Q}_p^\times$, this isomorphism identifies $E_d(\mathbf{Q}_p)$ with $E_{d'}(\mathbf{Q}_p)$ and by the definition of $c_p(d)$ we get $c_p(d) = c_p(d')$. □

By Lemma 4(i), every quadratic twist E_d of E is a twist by some (unique) squarefree integer. From now on we will assume that d is a squarefree integer.

Proposition 5. Suppose p is a prime not dividing 2Δ. If $p \nmid d$ then $c_p(d) = 1$. If $p \mid d$, then

$$c_p(d) = 1 + \#\{\text{roots of } f(x) \equiv 0 \pmod{p} \text{ in } \mathbf{Z}/p\mathbf{Z}\} = 1,\ 2, \text{ or } 4.$$

Proof. If $p \nmid 2\Delta d$ then E_d has good reduction at p, so $c_p(d) = 1$. If $p \mid d$ but $p \nmid 2\Delta$ then we are in case 6 of Tate's algorithm [T]. □

Note that for every p not dividing 2Δ, the number of roots of $f(x)$ modulo p is at least as large as the number of roots of $f(x)$ in $\mathbf{Q}$. Thus if $p \mid d$ and $p \nmid 2\Delta$, then $c_p(d) \geq \#E(\mathbf{Q})[2]$.

If $p \mid 2\Delta$ the situation is more complicated. However, for those primes, to determine $c_p(d)$ for every d, Lemma 4(ii) shows that it is enough to compute $c_p(d)$ (using Tate's algorithm) for d in a set of representatives of $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$. Note that $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$ has order 4 if $p > 2$, and order 8 if $p = 2$.

Example 6. $E : y^2 = x^3 - x$

We have $\Delta = 64$, and $x^3 - x$ factors into linear factors over $\mathbf{Q}$, so Proposition 5 shows that for $p > 2$ we have

$$c_p(d) = \begin{cases} 1 & \text{if } p \nmid d, \\ 4 & \text{if } p \mid d. \end{cases} \tag{1}$$

Tate's algorithm (cases 4 and 7.2, respectively) gives

$$c_2(d) = \begin{cases} 2 & \text{if } 2 \nmid d, \\ 4 & \text{if } 2 \mid d. \end{cases} \tag{2}$$

(Alternatively, we can use PARI/GP to compute that

$$c_2(1) = c_2(3) = c_2(-1) = c_2(-3) = 2,$$
$$c_2(2) = c_2(6) = c_2(-2) = c_2(-6) = 4,$$

and then use Lemma 4(ii) to deduce (2).)

Combining (1) and (2) we conclude that

$$\prod_p c_p(d) = \begin{cases} 2^{2\omega(d)+1} & \text{if } d \text{ is odd,} \\ 2^{2\omega(d)} & \text{if } d \text{ is even,} \end{cases}$$

where $\omega(d)$ is the number of prime divisors of d.

Example 7. $E : y^2 + y = x^3 - x^2 - 10x - 20$

This is the modular curve $X_0(11)$, with discriminant -11^5. We will use the model (not minimal at 2)

$$y^2 = x^3 - 4x^2 - 160x - 1264$$

with discriminant $\Delta = -2^{12}11^5$. For $p \neq 2, 11$, Proposition 5 shows that

$$c_p(d) = \begin{cases} 1 & \text{if } p \nmid d, \\ 1 + \#\{\text{roots of } x^3 - 4x^2 - 160x - 1264 \bmod p\} & \text{if } p \mid d. \end{cases}$$

Since $x^3 - 4x^2 - 160x - 1264$ is irreducible over $\mathbf{Q}$, $c_p(d)$ can be 1, 2, or 4. More precisely, the Galois group of $x^3 - 4x^2 - 160x - 1264$ over $\mathbf{Q}$ is S_3, so the Cebotarev theorem shows that if D_k is the density of the set of primes p such that $x^3 - 4x^2 - 160x - 1264$ has k roots modulo p, then $D_0 = 1/3$, $D_1 = 1/2$, and $D_3 = 1/6$.

We also compute

d	1	3	−1	−3	2	6	−2	−6
$c_2(d)$	1	1	1	1	1	1	1	1

d	1	−1	11	−11
$c_{11}(d)$	5	1	4	2

Therefore by Lemma 4(ii), $c_2(d) = 1$ for every d, and

$$c_{11}(d) = \begin{cases} 5 & \text{if } d \text{ is a nonzero square modulo 11,} \\ 1 & \text{if } d \text{ is not a square modulo 11,} \\ 4 & \text{if } 11 \mid d \text{ and } \frac{d}{11} \text{ is a square modulo 11,} \\ 2 & \text{if } 11 \mid d \text{ and } \frac{d}{11} \text{ is not a square modulo 11.} \end{cases}$$

References

[S] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **151**, New York: Springer-Verlag (1994).

[T] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable (IV), *Lecture Notes in Math.* **476**, New York: Springer-Verlag (1975) 33–52.

Department of Mathematics,
Stanford University,
Stanford, CA
94305 USA