Rank determines semi-stable conductor

H. Kisilevsky¹

Department of Mathematics and Statistics and CICMA, Concordia University, 1455 de Maisonneuve Blvd.
West, Montréal, Quebec, Canada H3G 1M8

Received 5 February 2003; revised 6 May 2003; accepted 1 July 2003

Communicated by D. Goss

Abstract

Suppose that $E_1$ and $E_2$ are elliptic curves over the rational field, $\mathbb{Q}$, such that $\text{ord}_s L(E_i/K, s) \equiv \text{ord}_s L(E_2/K, s) \pmod{2}$ for all quadratic fields $K/\mathbb{Q}$. We prove that their conductors $N(E_1)$ and $N(E_2)$ are equal up to squares. If $\text{rank}_2(E_1(K)) \equiv \text{rank}_2(E_2(K)) \pmod{2}$ for all quadratic fields $K/\mathbb{Q}$, then the same conclusion holds, provided the 2-parts of their Tate–Shafarevich groups are finite.

[© 2003 Elsevier Inc. All rights reserved.]

Y. Zarhin posed the following question:

Suppose that $X_1$ and $X_2$ are abelian varieties defined and isogenous over a number field $k$. Then for any finite extension field $K/k$,

$$\text{rank}_2(X_1(K)) = \text{rank}_2(X_2(K)).$$

(Here $\text{rank}_2(X(K))$ is the number of free generators of the Mordell–Weil group $X(K)$.) Zarhin’s question is whether the converse holds: Let $X_1$ and $X_2$ be abelian varieties defined over $k$. If $\text{rank}_2(X_1(K)) = \text{rank}_2(X_1(K))$ for every finite extension $K/k$, then are $X_1$ and $X_2$ isogenous over $k$?

In this article we consider this question for elliptic curves $E_1$ and $E_2$ defined over the rational field $\mathbb{Q}$. For an elliptic curve $E$, and for finite extensions $K/\mathbb{Q}$, $L(E/K, s)$ will denote the $L$-function of $E$ viewed as a curve over $K$.

By the recent proof [B-C-D-T, T-W, W] of the modularity of elliptic curves over $\mathbb{Q}$, we know that $L(E/\mathbb{Q}, s)$ has an analytic continuation for all $s \in \mathbb{C}$, and satisfies the

---

¹This work was supported in part by grants from NSERC and FCAR.

E-mail address: kisilev@mathstat.concordia.ca.
The Birch and Swinnerton-Dyer conjecture asserts that
\[ \text{ord}_{s=1}L(E/K, s) = \text{rank}_\mathbb{Z}(E(K)), \]
and that the Tate–Shafarevich group \( \text{III}(K) \) is finite. The “parity conjecture” for \( E \) asserts that
\[ \text{ord}_{s=1}L(E/K, s) \equiv \text{rank}_\mathbb{Z}(E(K)) \pmod{2}. \]

We note that \( \text{ord}_{s=1}L(E/K, s) \) is sometimes referred to as the “analytic rank” of \( E \) over \( K \). In view of Faltings’ Theorem, we can rephrase Zarhin’s question in terms of the analytic rank of \( E \) over \( K \) viz., Given elliptic curves \( E_1 \) and \( E_2 \) defined over \( \mathbb{Q} \) such that
\[ \text{ord}_{s=1}L(E_1/K, s) = \text{ord}_{s=1}L(E_2/K, s) \]
for all finite extensions \( K/\mathbb{Q} \), is it true that
\[ L(E_1/\mathbb{Q}, s) = L(E_2/\mathbb{Q}, s) ? \]

It is a pleasure to thank Ken Kramer for a number of valuable discussions regarding this paper and Karl Rubin for several useful suggestions.

**Theorem 1.** Let \( E_1 \) and \( E_2 \) be elliptic curves defined over \( \mathbb{Q} \), with conductors \( N(E_1) \) and \( N(E_2) \). Suppose that for every number field \( K \) with \( [K: \mathbb{Q}] \leq 2 \)
\[ \text{ord}_{s=1}L(E_1/K, s) \equiv \text{ord}_{s=1}L(E_2/K, s) \pmod{2}. \]
Then \( N(E_1) \) and \( N(E_2) \) are equal up to square factors.

**Proof.** Since the curves \( E_i \) are modular, their \( L \)-functions, \( L(E_i/\mathbb{Q}, s) \), have analytic continuations to the entire plane and satisfy functional equations. Consider the twists of the curves \( E_i \) by fundamental discriminants \( D \) of quadratic fields which are coprime to \( N(E_1)N(E_2) \). For such a discriminant \( D \), let \( K = \mathbb{Q}(\sqrt{D}) \), let \( E_i^{(D)} \) denote the twisted curves, and let \( L(E_i^{(D)}/\mathbb{Q}, s) \) be the corresponding \( L \)-functions. Then \( L(E_i^{(D)}/\mathbb{Q}, s) \) is the twist of \( L(E_i/\mathbb{Q}, s) \) by the quadratic Dirichlet character \( \chi_D \) corresponding to \( K \), and is modular by Hecke’s theorem.

Since
\[ \text{ord}_{s=1}L(E_1/\mathbb{Q}, s) \equiv \text{ord}_{s=1}L(E_2/\mathbb{Q}, s) \pmod{2} \]
it follows that $L(E_1/Q, s)$ and $L(E_2/Q, s)$ have the same signs in their functional equations.

Also, by assumption we have

$$\text{ord}_s L(E_1/K, s) \equiv \text{ord}_s L(E_2/K, s) \pmod{2}.$$ 

Since

$$L(E_i/K, s) = L(E_i/Q, s)L(E_i^{(D)}/Q, s),$$

it follows that

$$\text{ord}_s L(E_1^{(D)}/Q, s) \equiv \text{ord}_s L(E_2^{(D)}/Q, s) \pmod{2}$$

for all such fundamental discriminants $D$. Applying the functional equations [Sh, Theorem 3.66] to the $L$-functions $L(E_i^{(D)}/Q, s)$ we see that the sign of the functional equation for $L(E_i^{(D)}/Q, s)$ changes from that of $L(E_i/Q, s)$ by the factor $\chi_D(-N(E_i))$ and therefore

$$\chi_D(-N(E_1)) = \chi_D(-N(E_2)).$$

Hence $\chi_D(N(E_1)N(E_2)) = 1$ for all such $D$, and this implies that $N(E_1)$ and $N(E_2)$ are equal up to square factors. 

\textbf{Theorem 2.} Let $E_1$ and $E_2$ be elliptic curves defined over $\mathbb{Q}$, with conductors $N(E_1)$ and $N(E_2)$. Suppose that for every number field $K$ with $[K : \mathbb{Q}] \leq 2$

$$\text{rank}_E(E_1(K)) \equiv \text{rank}_E(E_2(K)) \pmod{2}.$$ 

If the 2-primary parts of Tate–Shafarevich groups, $\text{III}_2(E_i(K))$, are finite for all such $K$, then $N(E_1)$ and $N(E_2)$ are equal up to square factors.

\textbf{Proof.} Let $E$ be an elliptic curve defined over $\mathbb{Q}$. The main result of Monsky [Mo, Theorem 1.5] is that the “2-Selmer rank”, $s_2(E(K)) = \text{rank}_E E(K) + \dim_{\mathbb{F}_2} \text{III}_2(E(K))$ has the same parity as $\text{ord}_{s=1} L(E/K, s)$. But then if $\text{III}_2(E(K))$ is finite it follows that $\dim_{\mathbb{F}_2} \text{III}_2(E(K))$ is even and hence

$$\text{rank}_E E(K) \equiv \text{ord}_{s=1} L(E/K, s) \pmod{2}.$$ 

Therefore the finiteness of $\text{III}_2(E_i(K))$, together with the assumption

$$\text{rank}_E(E_1(K)) \equiv \text{rank}_E(E_2(K)) \pmod{2}$$

implies that

$$\text{ord}_{s=1} L(E_1^{(D)}/Q, s) \equiv \text{ord}_{s=1} L(E_2^{(D)}/Q, s) \pmod{2},$$
and so Theorem 1 gives the conclusion that $N(E_1)$ and $N(E_2)$ are equal up to square factors. 

**Corollary 1.** Suppose that $E_1$ and $E_2$ are semi-stable elliptic curves defined over $\mathbb{Q}$ such that

$$\text{ord}_{s=1} L(E_1/K, s) \equiv \text{ord}_{s=1} L(E_2/K, s) \pmod{2}$$

for all extensions $K/\mathbb{Q}$, with $[K: \mathbb{Q}] \leq 2$, then $N(E_1) = N(E_2)$. In particular, there are only a finite number of isogeny classes of such elliptic curves.

**Proof.** For semi-stable curves over $\mathbb{Q}$, the results of Wiles [W] and Taylor–Wiles [T-W] imply the modularity of the $E_i$. Then Theorem 1 shows that $N(E_1) = N(E_2)$ since they are both square-free.

**Corollary 2.** Suppose that $E_1$ and $E_2$ are semi-stable elliptic curves defined over $\mathbb{Q}$ such that

$$\text{rank}_\mathbb{Z}(E_1(K)) \equiv \text{rank}_\mathbb{Z}(E_2(K)) \pmod{2}$$

for all extensions $K/\mathbb{Q}$, with $[K: \mathbb{Q}] \leq 2$. If in addition, we assume that $\text{III}_2(E_i(K))$ is finite for all such $K$, then $N(E_1) = N(E_2)$. In particular, there are only a finite number of isogeny classes of such elliptic curves.

**Proof.** Corollary 2 follows from Theorem 2 as above.

We next construct some examples of nonisogenous elliptic curves to indicate that we cannot expect this approach to yield much more information on Zarhin’s conjecture. Specifically, we will give examples of elliptic curves $E_1$ and $E_2$, defined over $\mathbb{Q}$, with the same conductor $N = N(E_i)$, and which have the following property:

$$\text{rank}_\mathbb{Z}(E_1(K)) \equiv \text{rank}_\mathbb{Z}(E_2(K)) \pmod{2}$$

for all Galois extensions $K/\mathbb{Q}$ in which 2 is unramified, provided that the 2-primary parts of their Tate–Shafarevich groups, $\text{III}_2(E_i(K))$, are finite. (Conjecturally they will have ranks of the same parity for all finite extensions $K/\mathbb{Q}$.) Furthermore, the elliptic curves $E_1$ and $E_2$ also have the property that:

$$\text{ord}_{s=1} L(E_1/K, s) \equiv \text{ord}_{s=1} L(E_2/K, s) \pmod{2}$$

for all solvable extensions $K/\mathbb{Q}$. (Conjecturally they have analytic ranks of the same parity for all finite extensions $K/\mathbb{Q}$.)

The change of parity of both the algebraic rank and the analytic rank in quadratic extensions was studied by Kramer [K] and Kramer–Tunnell [K-Tu].

**Theorem 3.** Let $E_1$ and $E_2$ be semi-stable elliptic curves defined over a number field $k$ such that $E_1$ and $E_2$ have the same reduction type (good reduction, split multiplicative reduction, or nonsplit multiplicative reduction) at all primes $p$ of $k$. Suppose that $E_1$
and $E_2$ have models over $k$ with equal discriminants. Let $K/k$ be a quadratic extension.

(1) (Kramer) Suppose that the prime 2 is not ramified in $k$ and that the 2-primary parts of the Tate–Shafarevich groups, $\Sha_2(E_i(K))$, are finite, then

$$\text{rank}_\mathbb{Z}(E_1(K)) \equiv \text{rank}_\mathbb{Z}(E_2(K)) \pmod{2}.$$  

(2) (Kramer–Tunnell) The elliptic curves $E_1/K$ and $E_2/K$ have the same local $\varepsilon$-factors.

Proof. The statement (1) is proved by Kramer [K, Section 4, Theorem 1 and Corollary 2]. Assuming that $\Sha_2(E_i(K))$ is finite, he computes the parity of $\text{rank}_\mathbb{Z}(E_i(K))$ only in terms of primes of $K$ at which $E_i$ has split multiplicative reduction and the quadratic character of $K/k$. But since these are the same for $E_1$ and $E_2$ under our hypotheses, the first conclusion follows.

Statement (2) is a consequence of Theorem 4.4, Section 4 of Kramer–Tunnell [K-Tu]. Here they show that for a semi-stable elliptic curve $E$, the local $\varepsilon$-factors of $E/K$ at a prime $\mathfrak{p}$, can be calculated in terms of the quadratic character of $K/k$ at $\mathfrak{p}$ evaluated on the discriminant of $E$, and a local norm index which is computed in Kramer [K, pp. 127–128], also in terms of the discriminant of $E$ and the reduction type of $E$ at $\mathfrak{p}$. Since the discriminants of $E_1$ and $E_2$ were assumed to be equal, and they had the same reduction type at all primes $\mathfrak{p}$ of $K$, their local $\varepsilon$-factors over $K$ agree. □

We first consider the algebraic rank, $\text{rank}_\mathbb{Z}(E_i(K))$ for Galois extensions $K/\mathbb{Q}$ unramified at 2. We need the following:

**Proposition 1.** Suppose that $V$ is a finite dimensional $\mathbb{Q}$-vector space which admits an action of a finite group $G$ of odd order. Then

$$\dim V \equiv \dim V^G \pmod{2}.$$  

**Proof.** This is true for cyclic groups of odd prime order as the only irreducible representations are the trivial representation and the augmentation representation. The result follows by solvability of groups of odd order. Alternatively, it is an exercise in Serre [S, pp. 109–110] that every nontrivial irreducible character of a group of odd order is complex, and hence can be paired with its conjugate. It then is clear that the parity of the degree of the representation $\rho$, determined by the action of $G$ on $V$ is equal to the parity of the multiplicity of the trivial representation $\chi_0$ in $\rho$. □

**Corollary 3.** If $E$ is an elliptic curve defined over a field $k$ and $K/k$ is a Galois extension of odd degree then

$$\text{rank}_\mathbb{Z}(E(K)) \equiv \text{rank}_\mathbb{Z}(E(k)) \pmod{2}$$

as long as both are finite.
Proof. Setting $V = E(K) \otimes \mathbb{Q}$ and $G = \text{Gal}(K/k)$ the result follows from Proposition 1. □

Therefore we have:

**Theorem 4.** Suppose that $E_1$ and $E_2$ are semi-stable elliptic curves defined over $\mathbb{Q}$ with the same conductor $N$. Assume that $E_1$ and $E_2$ both have the same multiplicative reduction type (split or nonsplit) at all primes dividing $N$. If

$$\text{rank}_{\mathbb{Z}}(E_1(\mathbb{Q})) \equiv \text{rank}_{\mathbb{Z}}(E_2(\mathbb{Q})) \pmod{2}$$

then

$$\text{rank}_{\mathbb{Z}}(E_1(K)) \equiv \text{rank}_{\mathbb{Z}}(E_2(K)) \pmod{2}$$

for all Galois extensions $K/\mathbb{Q}$ unramified at 2 provided that the groups $\text{III}_2(E_i(K))$ are finite.

Proof. Since nonsplit reduction becomes split over a field $k$ if and only if the completion of $k$ contains the unramified quadratic extension of $\mathbb{Q}_p$, the reduction type depends only on $k$, not on the curve. Thus $E_1$ and $E_2$ have the same reduction type over every $k$.

Let $K/\mathbb{Q}$ be a Galois extension unramified at 2, and let $G = \text{Gal}(K/\mathbb{Q})$. If $K/\mathbb{Q}$ has odd degree, then Corollary 3 implies that the ranks of $E_1(K)$ and $E_2(K)$ have the same parity provided that the ranks of $E_1(\mathbb{Q})$ and $E_2(\mathbb{Q})$ have the same parity. If $K/\mathbb{Q}$ has even degree, then $G$ contains an element of order 2, and let $k_0$ denote its fixed field. Then $k_0/\mathbb{Q}$ is an extension unramified at 2, and it follows from Theorem 3 (1) that the ranks of $E_1(K)$ and $E_2(K)$ have the same parity provided that the groups $\text{III}_2(E_i(K))$ are finite. □

Now consider the analytic rank for solvable extensions.

**Proposition 2.** Let $k$ be a number field, and suppose that $K/k$ is a Galois extension of odd degree, with $\text{Gal}(K/k) = G$. Let $L(E/k,s)$ be the $L$-function of $E/k$, and $L(E/K,s)$ be that for $K/k$. If $L(E/k,s)$ is automorphic, then so is $L(E/K,s)$, and furthermore

$$\text{ord}_{s=1} L(E/K,s) \equiv \text{ord}_{s=1} L(E/k,s) \pmod{2}.$$ 

Proof. Since $G$ has odd order it is a solvable group. Hence, by induction, we may reduce the result to the case that $G$ is a cyclic group of prime order. Then the Base Change Theorem of Arthur–Clozel [A-C] asserts that the automorphy of $L(E/k,s)$ implies that of $L(E/K,s)$. Furthermore, in this case

$$L(E/K,s) = \prod_{\chi \in \hat{G}} L(E/k,\chi, s).$$
Since $L(E/k, s)$ is real for real $s$, it follows that the signs of the functional equations for $L(E/k, z, s)$ and $L(E/k, \bar{z}, s)$ are complex conjugates, and so have product equal to 1. Since $|G|$ is odd, we see that the sign of the functional equation for $L(E/K, s)$ is the same as that for $L(E/k, s)$ and hence
\[ \text{ord}_{s=1} L(E/Ks) \equiv \text{ord}_{s=1} L(E/k, s) \pmod{2}. \]

**Theorem 5.** Suppose that $E_1$ and $E_2$ are semi-stable elliptic curves defined over $\mathbb{Q}$ with the same minimal discriminant $\Delta$ and the same conductor $N$. Assume that $E_1$ and $E_2$ both have split multiplicative reduction at all primes dividing $N$. If
\[ \text{ord}_{s=1} L(E_1/\mathbb{Q}, s) \equiv \text{ord}_{s=1} L(E_2/\mathbb{Q}, s) \pmod{2} \]
then
\[ \text{ord}_{s=1} L(E_1/K, s) \equiv \text{ord}_{s=1} L(E_2/K, s) \pmod{2} \]
for all solvable extensions $K/\mathbb{Q}$.

**Proof.** Since the curves $E_i$ are semi-stable over $\mathbb{Q}$, Wiles [W] and Taylor–Wiles [T-W] imply that they are modular, and hence their $L$-functions, $L(E_i/\mathbb{Q}, s)$, are automorphic. Therefore, by Proposition 3, the $L$-functions, $L(E_i/K, s)$, are automorphic for any solvable extension $K/\mathbb{Q}$. Also, since $E_1$ and $E_2$ have the same discriminant, and since both have split multiplicative reduction at all primes dividing their common conductor, $N$, the same is true for any finite extension $k/\mathbb{Q}$. Therefore by Theorem 3(2) [K-Tu, Theorem 4.4, Section 4], we see that $E_1$ and $E_2$ have the same $\varepsilon$-factors over $K$, for every quadratic extension $K/k$. If in addition, $K/\mathbb{Q}$ is solvable, it follows from their automorphy that $L(E_i/K, s)$ have the same signs in their functional equations (see [J]). Therefore applying either Proposition 3 or Theorem 3(2) successively, it follows that if
\[ \text{ord}_{s=1} L(E_1/\mathbb{Q}, s) \equiv \text{ord}_{s=1} L(E_2/\mathbb{Q}, s) \pmod{2} \]
then
\[ \text{ord}_{s=1} L(E_1/K, s) \equiv \text{ord}_{s=1} L(E_2/K, s) \pmod{2} \]
for all solvable extensions $K/\mathbb{Q}$.

**Example** (Computed by J. Fearnley). $N = 307$. There are 4 nonisogenous curves (307A, 307B, 307C, and 307D) in Cremona’s tables [Cra] of conductor 307 and discriminant $-307$. All of them have rank 0 and split multiplicative reduction at $p = 307$. By Theorems 4 and 5, it follows that the above curves have analytic ranks of the same parity for all solvable extensions $K$ of $\mathbb{Q}$, and that their algebraic ranks have the same parity for all Galois extensions $K/\mathbb{Q}$ in which 2 is unramified provided that the 2-primary parts of their Tate–Shafarevich groups, $\Sha(2)(E_i(K))$, are finite.

Note that these curves do not provide counter-examples to Zarhin’s question. Twisting the first by $-7$ gives a curve of rank 2 (by Cremona’s Mrank program) and
$L(1) = 0$, by Kolyvagin [Ko], while the rest have rank 0 and nonvanishing $L$-function at $s = 1$.

$N = 1187$. There are 3 nonisogenous curves of conductor 1187 and discriminant $-1187$ of rank 0 and split multiplicative reduction at $p = 1187$. Twisting the first by $-43$ gives a curve of rank 2 and $L(1) = 0$, while the rest have rank 0 and nonvanishing $L$-function at $s = 1$.

References


