Ranks of twists of elliptic curves

(These are some notes to my Number Theory Seminar lecture Feb. 3, 2010)

B. Mazur

In this lecture I'll talk a bit more about Mordell-Weil stability, and discuss–in a slightly more precise way—my joint work with Karl Rubin, and specifically some of the contents of the article with Karl: "Ranks of twists of elliptic curves and Hilbert's Tenth Problem."

1. Mordell-Weil Stability

Let L/K be a finite extension of number fields. Does there exist an elliptic curve E over K with the property that

$$rank(E(K)) \ = \ rank(E(L)) > 0?$$

If so, then H10P has a negative solution for the rings of integers in any number field.

One does not need the full strength of the above statement. In fact,

Theorem 1.1. (Poonen, Shlapentokh, Eisenträger) if for every cyclic Galois number field extension of prime degree L/K there is an elliptic curve E over K with the property that

$$rank(E(K)) \ = \ rank(E(L)) > 0,$$

then

- H10P has a negative solution for any commutative ring of infinite cardinality that is finitely generated over $\mathbf{Z}$, and
- for K any number field if $\mathcal{O}_K$ is its ring of integers, every listable subset of $\mathcal{O}_K$ is Diophantine over $\mathcal{O}_K$.

Karl Rubin and I show that if the 2-adic Shafarevich-Tate Conjecture holds, then the hypotheses of Theorem 1.1 hold, and therefore, conditional on the 2-adic Shafarevich-Tate Conjecture, we see that, among other things, H10P has a negative solution for the ring of integers in any number field.

We do this by an analysis of 2-Selmer groups of elliptic curves.

2. Setting up

If E is an elliptic curve over a number field K we will be considering *Kummer* 2-*descent* for E over K, which has to do with the cohomology sequence corresponding to the exact sequence of G_K-modules

$$0 \to E[2] \to E \overset{\text{mult by } 2}{\longrightarrow} E \to 0.$$

One gets a natural injection of $\mathbf{F}_2$-vector spaces

$$E(K)/2E(K) \hookrightarrow H^1(G_K, E[2]).$$

Let us identify $E(K)/2E(K)$ with its image subspace of $H^1(G_K, E[2])$. We will assume the 2-adic Shafarevich-Tate Conjecture (STC) for all elliptic curves over all number fields.

2.1. Exponent 2 Selmer groups.

The vector space $H^1(G_K, E[2])$ is infinite dimensional, but there is a natural finite dimensional space in it that contains $E(K)/2E(K)$—and therefore that provides an upper bound for the rank of the Mordell-Weil group of E over K. Namely, for each place v of K, setting

$$H^1_f(K_v, E[2]) := \text{the image of } E(K_v)/2E(K_v) \hookrightarrow H^1(K_v, E[2])$$

we see that under the specialization mapping

$$H^1(K, E[2]) \to H^1(K_v, E[2])$$

the subspace $E(K)/2E(K)$ maps to $H^1_f(K_v, E[2]) \subset H^1(K_v, E[2])$. If we want to emphasize the place v we might write $H^1_f(K_v, E[2])$ as $H^1_{f_v}(K_v, E[2])$. Note though, the slight abuse of notation in that $H^1_f(K_v, E[2])$, as defined, depends upon E and not only on $E[2]$.

Nevertheless, and this is an important point of us, for places $v \not| 2\infty$ and such that E has good reduction at v[1] the subspace

$$H^1_f(K_v, E[2]) \subset H^1(K_v, E[2])$$

does not depend upon E, and only on $E[2]$ since (for these places v) this subspace is just the image

$$H^1(K_v^{\text{unr}}, E[2]) \longrightarrow H^1(K_v, E[2]).$$

Define, then, (the **exponent 2-Selmer group of E over K**)

$$S(K, E) \subset H^1(K, E[2])$$

[1] In particular, *for all but finitely many v*

to be the subspace consisting of cohomology classes $h \in H^1(K, E[2])$ such that for all places v of K the specialization of h to $H^1(K_v, E[2])$ lands in $H^1_f(K_v, E[2])$. By this discussion we have

$$E(K)/2E(K) \subset S(K, E) \subset H^1(K, E[2])$$

It is known that $S(K, E)$ is *finite dimensional,* and—equally significant—it is computable. Put

$$s(K, E) := \dim_{\mathbf{F}_2} S(K, E)$$

so that we have the upper bound:

$$s(K, E) \geq \mathit{rank}\ E(K).$$

One consequence of STC is that

$$s(K, E) \equiv \mathit{rank}\ E(K) \mod 2$$

so that if $s(K, E) = 1$ then, conditional on STC, $\mathit{rank}\ E(K) = 1$ as well.

2.2. **Quadratic twists.** If F/K is a quadratic extension, let E^F denote the elliptic curve over K obtained by twisting E with the quadratic character over K corresponding to F/K. Note that we have the all-important isomorphism,

$$E[2] = E^F[2],$$

which we use to identify these $\mathbf{F}_2[G_K]$-modules, and therefore we also have the identification

$$H^1(K, E[2]) = H^1(K, E^F[2]).$$

To be sure, the "local conditions" used to define the finite subspaces $S(K, E)$ and $S(K, E^F)$ in $H^1(K, E[2])$ may differ (but they can differ for only for finitely many places v). It follows, of course, that the exponent 2-Selmer groups $S(K, E)$ and $S(K, E^F)$ may differ as well. We work with this! (One can imagine a graph with vertices equal to the twists E^F and where any of the edges on this graph connect two twists where you can control the *change* in 2-Selmer rank: you move around in this graph.)

Definition 2.1. For E an elliptic curve over K and $s \geq \dim_{\mathbf{F}_2} E(K)[2]$ let $N_s(E, K; X)$ denote the number of quadratic extensions F/K with $\mathrm{d}\mathit{isc}(F/K) \leq X$ such that $s(K, E^F) = s$.

Definition 2.2. We'll say that E an elliptic curve over K has **constant 2-Selmer parity** if

$$s(K; E) \equiv s(K, E^F) \mod 2$$

for all quadratic extensions F/K.

Given a recent theorem of the Dokchitser brothers it is natural to conjecture that E over K has constant 2-Selmer parity if and only if K is totally imaginary and E acquires good reduction over an abelian extension of K. This is because T. and V. Dokchitser prove exactly this statement for analytic parity (as opposed to 2-Selmer parity)[2]. Also, in the light of various results for certain specific elliptic curves over $\mathbf{Q}$ (see section 4 below) it seems natural to conjecture that whenever there is one twist of E that has 2-Selmer rank s, the quantity of them[3] positive density of them that have 2-Selmer rank s. Specifically:

Conjecture 2.3. (**Positive Density**)

- If E has nonconstant parity over K then for any $s \geq \dim_{\mathbf{F}_2} E(K)[2]$ there is a positive density of twists of E with 2-Selmer rank s; i.e., there is a positive constant $\mathcal{C}_s = \mathcal{C}_s(K,E) > 0$ such that
$$N_s(E,K;X) = \mathcal{C}_s \cdot X + o(X).$$
- If E has constant parity over K then one has the same statement for the integers $s \geq \dim_{\mathbf{F}_2} E(K)[2]$ such that
$$s \;\equiv\; s(K,E) \quad \mod\; 2.$$

Our techniques seem not to be able to get results of this precision. But if you allow the phrase

"*E over K has many quadratic twists E^F with $s(K,E^F) = s$*"

to mean that $N_s(E,K;X) > X/log^{\alpha}X$ for some α and $X >> 0$ then we show, for example, that if L/K is an arbitrary Galois number field extension that is cyclic of prime degree, and if E is an elliptic curve over K satisfying our running hypotheses (see section 5 below) we have that for any $s \geq 0$ the elliptic curve E over K has many quadratic twists[4] E^F with $s(K,E^F) = s(L,E^F) = s$.

3. Further notes about "many twists" and "positive density"

Here is an example of two results that we prove unconditionally:

[2] T. Dokchitser, V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank* Acta Arithmetica **137** (2009) 193-197

[3] ordering these twists, say, by the size of $\mathrm{d}isc(F/K)$

[4] This number $a = 2/3$ or $a = 1/3$ according as the action of the Galois group on $E[2]$ is $\mathrm{GL}_2(\mathbf{F}_2)$ or cyclic of order three.

Theorem 3.1. Given any number field K there is an elliptic curve E over K such that there are many quadratic twists of E such that the twisted elliptic curve E^F has no nontrivial rational points over K.

We can even take E to be the base change to K of an elliptic curve over $\mathbf{Q}$.

Theorem 3.2. If K is not totally imaginary, and E is any elliptic curve over K with no nontrivial K-rational 2-torsion, there are many quadratic twists E^F such that have no nontrivial rational points over K.

"Many quadratic twists" can be taken to mean here $>> X/\log^{2/3}(X)$ if the action of the Galois group on $E[2]$ is the full $\mathrm{GL}_2(\mathbf{F}_2)$-action and $>> X/\log^{1/3}(X)$ if the action is cyclic of order three.

4. Positive density over the field $K = \mathbf{Q}$

There is an extensive literature about this topic. In this footnote[5] are some of the relevant references, and here are comments about a few of these articles[6].

Briefly,

- In [**HB**], Heath-Brown works with the elliptic curve

$$E : y^2 = x^3 - x$$

[5] *Some literature*

[**C**] S. Chang, Quadratic Twists of Elliptic Curves with Small Selmer Rank, (arXiv:0809.5019)

[**H-B**] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem II, Invent. Math. **118** (1994), 331370.

[**J-O**] K. James and K. Ono, Selmer groups of quadratic twists of elliptic curves, Math. Ann. **314** (1999), 117.

[**O**] K. Ono, Non-vanishing of quadratic twists of modular L-functions and applications to elliptic curves, J. reine angew. Math. **533** (2001), 8197.

O-S] K. Ono and C. Skinner, Non-vanishing of quadratic twists of modular L-functions, Invent. Math. **134** (1998), 651660.

[**S-D**] Sir Peter Swinnerton-Dyer, The effect of twisting on the 2-Selmer group, Math. Proc. Camb. Phil. Soc. **145** (2008), 513526.

[**X-Z**] M. Xing and A. Zaharescu, Distribution of Selmer groups of quadratic twists of a family of elliptic curves, Adv. Math. **219** (2008), 523553.

[**Y**] G. Yu, On the quadratic twists of a family of elliptic curves, Mathematika 52 (2005), 139154.

[6] For more, see the neatly listed and annotated survey of work regarding twists of elliptic curves over $\mathbf{Q}$ in the introduction of the article bf [S]

and computes $\mathcal{C}_s(\mathbf{Q}, E)$.

- In **[S-D]**, Swinnerton-Dyer also proves a theorem (of positive-density type. Computing the density by ordering twists in terms of the number of prime divisors of the discriminant, Swinnerton-Dyer shows that–in that sense of *density*—the density of twists (for the elliptic curves over $\mathbf{Q}$ that he is considering) with 2-Selmer rank s is
$$\frac{2^s \prod_{n=0}^{\infty}(1-2^{-2n-1})}{\prod_{j=1}^{k}(2^j-1)}.$$
It is interesting to note that— starting with these numbers as density—if one naively computes the "average number of elements in the group $S(\mathbf{Q}, E^F)$" (ordering twists of E in terms of the number of prime divisors of the discriminant) one gets the number 3, which is the same number that Manjul Bhargava has recently shown to be the average number of elements in the group $S(\mathbf{Q}, E)$ where E ranges now over all elliptic curves over $\mathbf{Q}$ ordered by Faltings height.
- In **[O-S]** Ken Ono and Chris Skinner proved (using Kolyvagin et al) a similar result to Theorem 3.2 (for $K = \mathbf{Q}$) by showing the analogous statement for central values of L functions, but their theorem is stronger since they show the number of twists to be of positive density, and—in fact—of density 1/2.
- In **[J-S]** Kevin James and Ken Ono have results for numbers of twists with small ℓ-Selmer rank over $\mathbf{Q}$.

5. Main Theorems

5.1. **Running Hypotheses:** Let K be a number field and E an elliptic curve over K with Δ_E a discriminant of a model of E over K. Our running hypotheses on E over K will be:

- The action of G_K on $E[2]$ is *full* in the sense that its splitting field is an S_3-extension of K.
- For some place v_o of K one of these two conditions hold:

  (1)
  - $v_o \nmid 2\infty$,
  - E has multiplicative reduction at v_o,
  - $\mathrm{ord}_{v_o}(\Delta_E)$ is odd.

  or:

  (2)
  - v_o is real,
  - $(\Delta_E)_{v_o} < 0$.

5.2. **The new part of 2-Selmer.** Let F/K be a quadratic extension and E^F the twist of E by the quadratic character determining F/K. Let $s(K,E)$ be the $\mathbf{F}_2$-dimension of the 2-Selmer group of E over K, viewed as $\mathbf{F}_2$-vector space.

If L/K is a cyclic extension of odd prime degree, define $s^{\mathrm{new}}(L,E)$ to be the $\mathbf{F}_2$-dimension of the "new part" of the Selmer $\mathbf{F}_2[Gal(L/K)]$ module $S(L,E)$ so that

$$s(L,E) = s(K,E) + s^{\mathrm{new}}(L,E).$$

5.3. **(Arbitrary Selmer 2-rank over K and L/K-stability of the new part).** Under the above running hypotheses, the following theorems hold.

Theorem 5.1. For L/K a given cyclic extension of odd prime degree[7] and for *any* $s \geq 0$, the elliptic curve E has "many" twists[8] E^F such that $s(K,E^F) = s$ and

$$s^{\mathrm{new}}(L,E^F) = s^{\mathrm{new}}(L,E).$$

We do this by single steps, showing that we can increase 2-Selmer rank by one, keeping the new part stable, and—if the 2-Selmer rank is positive, we can decrease it by one, also keeping the new part stable. If $Gal(L/K)$ is of odd prime order. let

$$\mathbf{F}_2[Gal(L/K)] = \mathbf{F}_2 \bigoplus \{\oplus_i k_i\}$$

where k_i are fields $(i = 1,2,\ldots,\nu)$ spanning the augmentation ideal of the group ring $\mathbf{F}_2[Gal(L/K)]$—allowing us to break up $S^{\mathrm{new}}(L,E)$ into a direct sum of k_i-vectors spaces:

$$S^{\mathrm{new}}(L,E) = \oplus_i S^{\{i\}}(L,E).$$

5.4. **(Reduction of the new part).** Writing

$$s^{\{i\}}(L,E) := \dim_{k_i} S^{\{i\}}(L,E),$$

we have the theorem:

Theorem 5.2. Keeping to the running hypotheses, suppose that L/K is a cyclic extension of odd prime degree, and that $s^{\{i\}}(L,E) \geq 1$ for all $i = 1,2,\ldots,\nu$. There is a quadratic twist E^F such that

$$s^{\{i\}}(L,E^F) = s^{\{i\}}(L,E) - 1$$

for $i = 1,2,\ldots,\nu$.

[7] We also show the analogous thing for the case of L/K quadratic, where the argument is slightly different.

[8] for the definition of this see the previous section

5.5. **Applications.** These theorems, put together give us the following corollary:

Corollary 5.3. Suppose L/K is a cyclic extension of odd prime degree[9]. Let $s \geq 0$. There is an elliptic curve A over K that is a quadratic twist of E and that has the following features:

- $s(K, A) = s$,
- $rank(A(L)) = rank(A(K))$.

This corollary follows by applying Theorem 5.2 repeatedly until we get a twist A' of E with $s^{\{i_o\}}(L, A') = 0$ for *some* i_o. Then use Theorem 5.2 to get a twist A of A' (and hence of E) which retains the fact that $s^{\{i_o\}}(L, A) = 0$ for some i, and also has $s(K, A) = s$. We must then show that $rank(A(L)) = rank(A(K))$. Noting that $A(L)$ is a $\mathbf{Z}[Gal(L/K)]$-module (and that $Gal(L/K)$ has odd prime degree) you prove that a strict inequality of ranks, $rank(A(L)) > rank(A(K))$, would imply that $s^{\{i\}}(L, A) > 0$ for all i. Therefore $rank(A(L)) = rank(A(K))$ and Corollary 5.4 is proved.

Corollary 5.4. Let K be any number field and E any elliptic curve over K that satisfies our running hypotheses. Let L/K be cyclic of prime order. Then there exists a quadratic twist A of E over K such that $rank(A(L)) = rank(A(K)) = 1$.

6. Methods

6.1. A simple Selmer Rank-Changing Lemma.

By the **troublesome places** for E an elliptic curve over K (satisfying our running hypotheses) we mean

- all primes of K where E has additive reduction,
- all primes of multiplicative reduction with $ord_v(\Delta_E)$ even,
- all primes above 2,
- all real places with $(\Delta_E)_v > 0$.

Let F/K be a quadratic extension such that:

- All troublesome places of K for E split in F/K,
- there is a unique finite prime v_o of K such that F/K is ramified at v_o, and $E(K_{v_o})[2] \neq 0$;
- the prime v_o has the added property that $H^1_{f_v}(K_v, E[2])$ is of dimension one.

[9] See footnote 1

Lemma 6.1. (**simple rank changing lemma**) Under the above hypotheses for F/K and the running hypotheses for E over K consider the localization mapping

$$\lambda := loc_{v_o} : S(K,E) \longrightarrow H^1_{f_v}(K_v, E[2]).$$

We have that $s(K,E^F) = s(K,E)+1$ if λ is zero,
and $s(K,E^F) = s(K,E)-1$ if λ is nonzero.

The "edges" of one of the graphs alluded to in the earlier sections connect twists of E that allow us to pass from one vertex to the other using the hypotheses of this simple rank changing lemma[10]. We will, later, give a sense of what goes into the proof of this type of "rank-changing lemma" but, for now, I only want to point out that it won't yet give us the type of Mordell-Weil stability theorem that we are after, since the designated v_o in K may very well split in the cyclic extension L/K. We need a similar lemma involving more than one v_o, and more general hypotheses.

6.2. **A more general Selmer Rank-Changing Lemma.**

Let T be a finite set of places of K and consider the direct sum of the local finite cohomology groups, $H^1_{f_v}(K_v, E[2])$, for $v \in T$; i.e.:

$$H_T := \sum_{v \in T} H^1_{f_v}(K_v, E[2]).$$

We have a natural mapping

$$loc_T : S(K,E) \to H_T$$

and let $\epsilon_T(E,K)$ denote the dimension of the cokernel of this mapping. Now let F/K be a quadratic extension such that all troublesome places of K for E split in F/K and $\epsilon_T(E,K) \leq 1$.

Global (Poitou-Tate) duality together with some very interesting congruence (mod 2) due to Kramer, together with an application of Cebotarev, gives us, among other things, that

$$s(K,E^F) = s(K,E) - \dim H_T + 2\epsilon_T(E,K).$$

(The argument for this also makes use of the useful trivia fact: if you know the parity of a non-negative number ≤ 1, then you know

[10] we may also add edges where we can control the change in 2-Selmer rank by other means ...

the number.) It is this type of rank-changing lemma that will allow us, under suitable conditions, to control the change of rank of both $s(K, E)$ and $s(L, E)$ after twist to E^F.

6.3. **Kramer's Congruences.** Let F/K be a quadratic extension of number fields and put

$$N_v^F := \text{the image of } E(F_w) \overset{Norm}{\longrightarrow} E(K_v)$$

for w a place of F over v. Put

$$\delta_v^F := \dim \frac{E(K_v)}{N_v^F}$$

(these being a.e. zero).

Lemma 6.2. Identifying

$$H^1_{f_v}(K_v, E[2]) = E(K_v)/2E(K_v)$$

we have

$$H^1_{f_v}(K_v, E[2]) \cap H^1_{f_v}(K_v, E^F[2]) = N_v^F/2E(K_v).$$

Theorem 6.3. (**Kramer**)

$$s(K, E^F) \equiv s(K, E) + \sum_v \delta_v^F \mod 2.$$

Give idea of the unusual proof!

Kramer defines an alternating pairing on

$$S(K, E^F) \cap S(K, E) \subset H^1(K, E[2])$$

with kernel equal to $N_{F/K}S(K, F)$. So we have that the parity of the dimensions of $S(K, E^F) \cap S(K, E)$ and $N_{F/K}S(K, F)$ are the same; this gives him the basic congruence modulo two necessary for showing the formula above.

6.4. **Criteria for change or no change in local conditions defining the Selmer group of a twist of E.** From the lemma and other arguments you get fairly sharp criteria for when a twist induces no change in local conditions at a given place v and when it induces transversal change. To give a sense of the type of criteria, here is an example (where there is no change):

Lemma 6.4. If at least one of the following conditions holds, then

$$H^1_{f_v}(K_v, E[2]) = H^1_f(K_v, E^F[2])$$

and $\delta_v^F = 0$

(1) v splits in F/K, or

(2) $v \not| 2$ and $E(K_v)[2] = 0$, or
(3) E has multiplicative reduction at v, F/K is unramified at v, and $ord_v(\Delta_E)$ is odd, or
(4) v is real and $(\Delta_E)_v < 0$, or
(5) v is a "good" prime, in the sense that E has good reduction at v and F/K is unramified at v.

In contrast to the above lemma, we get a change of local condition and in fact, *transversality* in the sense that

$$H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2]) = 0$$

and

$$E(K_v)/Norm_{F/K}E(F_w) \cong H^1_f(K_v, E[2]),$$

if $v \not| 2\infty$, v is *ramified* in F/K and E has good reduction at v.

6.5. **Global Duality.** Let T be a finite set of places of K and consider the direct sum of the local finite cohomology groups, $H^1_{f_v}(K_v, E[2])$, for $v \in T$; i.e.:

$$H_T := \sum_{v \in T} H^1_{f_v}(K_v, E[2]).$$

We have a natural mapping

$$loc_T : S(K, E) \to H_T$$

and let $\epsilon_T(E, K)$ denote the dimension of the cokernel of this mapping.

Global duality gives us, among other things, that if a certain collection of places[11] of K split in F/K and if

(1) T is the set of finite primes v of K such that F/K is ramified and and $E(K_v)[2] \neq 0$, and
(2) $\epsilon_T(E, K) \leq 1$,

then:

$$s(K, E^F) = s(K, E) - \dim H_T + 2\epsilon_T(E, K).$$

[11] These are:

- all primes of E of additive reduction,
- all primes of multiplicative reduction with $ord_v(\Delta_E)$ even,
- all primes above 2,
- all real places with $(\Delta_E)_v > 0$.

(The argument for this also makes use of the useful trivia fact: if you know the parity of a non-negative number ≤ 1, then you know the number.)

6.6. **The Cebotarev density Theorem.** In order to apply the above formula, one has to find a pair $(F/K, T)$ where F/K is a quadratic extension and T is a subset of ramified places of F/K satisfying the maze of conditions above. In most of our applications—e.g. proceeding by *by single steps* in Theorem 5.1—the set T will in fact consist in a single place corresponding to a prime ideal P, and $F = K(\sqrt{\pi})$ where π is a generator of an appropriate odd power of P pinned down by a number of further congruences. To guarantee the existence (and also to compute *densities* of appropriate such prime ideals P) we use, of course, Cebotarev's density Theorem.

It is at this point, by the way, that we make use of our *running hypotheses*; we need these hypotheses in order to guarantee that our Cebotarev conditions are satisfiable. We need that $K(E[2])$ is not contained in a certain elementary abelian 2-extension of K, so we have to assume $E(K)$ has no 2-torsion. Our running hypotheses 3.1 are also used here; without those hypotheses there are curves for which all twists have *the same 2-Selmer rank parity.*

7. A bit more detail: For fixed Galois extension L/K of prime degree, how to choose appropriate E so that we can get twists of E over K with different 2-Selmer ranks, *and* rank $E(K) =$ rank $E(L)$

Given an L/K cyclic of odd prime order p and E over K, and put $G = \mathrm{Gal}(L/K)$. We will be dealing with the group rings $R[G]$ for R various commutative rings. Let $I = I_R \subset R[G]$ denote the augmentation ideal, noting that $R = R[G]/I_R$. We view $S_2(E; L)$ as an $\mathbf{F}_2[G]$-module, which seems awkward at first, since $A := \mathbf{F}_2[G]$ is an étale $\mathbf{F}_2$-algebra, but not—of course—a field. We write it as as a direct product of fields, signaling out the "'first factor" as the quotient by the augmentation ideal, as follows:

$$A = \mathbf{F}_2[G] \;=\; \mathbf{F}_2 \times I_A \;=\; \mathbf{F}_2 \times k_1 \times k_2 \times \cdots \times k_\nu .$$

Note: If for some index $1 \leq i \leq \nu$ the k_i-vector space $S_2(E; L) \otimes_A k_i$ vanishes, then E has stable Mordell-Weil rank for the cyclic extension L/K. This is because there are only two $\mathbf{Q}$-rational irreducible factors of the group ring, $\mathbf{Q}[G] = \mathbf{Q} \oplus \mathbf{Q}[\mu_p]$ and so we see that if $E(L)$ is of rank strictly greater than the rank of $E(K)$ we must have that $E(L) \otimes \mathbf{Q}$ contains a (direct summand) sub-$\mathbf{Q}[G]$-module isomorphic to the augmentation ideal $I_{\mathbf{Q}}[G]$ and so $E(L) \otimes \mathbf{Q}_2$ contains a (direct summand) sub-$\mathbf{Q}_2[G]$-module isomorphic to the augmentation ideal $I_{\mathbf{Q}_2}[G]$ and therefore $E(L) \otimes \mathbf{Z}_2$ contains a sub-$\mathbf{Z}_2[G]$-module isomorphic to the augmentation ideal $I_{\mathbf{Z}_2}[G]$. It follows (by an easy argument) that we must have that $E(L) \otimes \mathbf{F}_2$ contains a submodule isomorphic to I_A and therefore that $S_2(E; L) \otimes_A k_i$ doesn't vanish for any i.

7.1. **Key Proposition.**

Proposition 7.1. Let K be a number field and E an elliptic curve over K with full Galois action on 2-torsion. Let Δ be the discriminant of some model of E and suppose that K has a place v_o satisfying one of the following conditions:

- v_o is real and $\Delta_{v_o} < 0$,
- v_o is nonarchimedean and doesn't divide 2, E has multiplicative reduction at v_o, and $\mathrm{ord}_{v_o}(\Delta)$ is odd.

Then:

(1) For every $r \geq 0$ E has"many" quadratic twists E' over K with 2-Selmer rank r.

(2) Let L/K be a cyclic extension of odd prime degree, with notation as above, and suppose that

$$S_2(E; L) \otimes_A k_i \neq 0$$

for all i $(0 \leq i \leq \nu)$.

Then there exists a quadratic twist E' of E such that

$$\dim_{k_i}\ S_2(E'; L) \otimes_A k_i \ = \ \dim_{k_i}\ S_2(E'; L) \otimes_A k_i \ - \ 1$$

for all i $(0 \leq i \leq \nu)$.

Proposition 7.1(1) is moving in the direction of at least a weak qualitative version of Conjecture 2.3. A further result which gives us some "mobility" for a general number field K and any elliptic curve E over K with no K-rational 2-torsion, is the following:

Proposition 7.2. If the rank of the 2-Selmer group of E is s we can achieve ranks s' by appropriate twists of E for any $s' \equiv s \mod 2$ such that

$$0 \leq s' \leq s.$$

That is, we can go down, preserving parity, in general (given that there is no 2-torsion rational over K). But—so far we can not "go up" in complete generality.