Isogeny invariance of the BSD conjecture

Akshay Venkatesh *

October 30, 2015

1 Examples

The BSD conjecture predicts that for an elliptic curve $E$ over $\mathbb{Q}$ with $E(\mathbb{Q})$ of rank $r \geq 0$,

$$
\frac{L^{(r)}(1, E)}{r!} = \frac{(\prod_p c_p)\Omega_E \cdot \#E(\mathbb{Q})_{\text{tor}} \#\hat{E}(\mathbb{Q})_{\text{tor}}^{\#}}{\#E(\mathbb{Q})_{\text{tor}} \#\hat{E}(\mathbb{Q})_{\text{tor}}} \quad (1.1)
$$

where

- $\hat{E}$ is the dual elliptic curve (so $\hat{E} \simeq E$, unlike for higher dimensions in general),
- $\Omega = \int_{E(\mathbb{R})} |\omega|$, and $\omega$ is the global section of $\Omega_{N(E)/\mathbb{Z}}^1$ corresponding to a choice of basis of the $\mathbb{Z}$-line $\text{Cot}_0(N(E))$ for the Néron model $N(E)$ of $E$ over $\mathbb{Z}$,
- $c_p$ is the number of connected components of $N(E)_{\mathbb{F}_p}$ that are geometrically connected over $\mathbb{F}_p$, or equivalently (by Lang’s theorem applied to $N(E)^0_{\mathbb{F}_p}$-torsors) have a rational point, so $c_p$ coincides with the number of $\mathbb{F}_p$-points of the finite étale component group $N(E)_{\mathbb{F}_p}/N(E)^0_{\mathbb{F}_p}$,
- $R_E$ is a regulator term that equals 1 when $E(\mathbb{Q})$ is finite.

We consider the three elliptic curves over $\mathbb{Q}$ with conductor 11:

1. $E_1 : y^2 + y = x^3 - x^2$, which happens to be $X_1(11)$,
2. $E_2 : y^2 + y = x^3 - x^2 - 10x - 20$, which happens to be $X_0(11)$,
3. $E_3 : y^2 + y = x^3 - x^2 - 7820x - 263580$.

These are all minimal Weierstrass models, so their smooth loci over $\mathbb{Z}$ are the relative identity components of the Néron models. The evident action of $(\mathbb{Z}/11\mathbb{Z})^\times$ on the fine moduli scheme $X_1(11)$ makes $\{\pm 1\}$ act trivially, and the resulting action of

*Notes by Tony Feng
the cyclic group $C = (\mathbb{Z}/11\mathbb{Z})^\times/\{\pm 1\}$ on $X_1(11)$ leaves invariant the forgetful map $X_1(11) \to X_0(11)$. The resulting map $X_1(11)/C \to X_0(11)$ between smooth projective (geometrically connected) curves is clearly bijective on $\mathbb{Q}$-points away from $j = 0, 1728$, so it is birational and hence an isomorphism. In other words, we have a natural 5-isogeny $E_1 \to E_2$.

To understand this isogeny in another way, we consider the moduli-theoretic viewpoint. By moduli-theoretic considerations, the two geometric cusps on $E_2$ (corresponding to the 11-gon and 1-gon equipped with their unique order-11 ample cyclic subgroups take up to automorphism of the polygon) are both $\mathbb{Q}$-points, and 5 of geometric cusps on $E_1$ are $\mathbb{Q}$-points (namely, the ones corresponding to the 11-gon equipped with a generator of its component group $\mathbb{Z}/11\mathbb{Z}$ up to sign). On $E_1$ with the model above, these are the points $\{(0,0), (0,-1), (1,0), (1,-1), \infty\}$. This exhausts $E_1(\mathbb{Q})$.

Remark 1.1. The fact that $E_1(\mathbb{Q})$ consists entirely of cusps reflects the fact that no elliptic curves over $\mathbb{Q}$ have a rational 11-torsion point.

Using the rational cusp for the 11-gon as the identity for the group law turns $X_0(11)$ (so not the cusp $\infty$ in the standard analytic modell) turns it into the elliptic curves $E_2$, and likewise for $E_1$ using any of the $\mathbb{Q}$-cusps on $X_1(11)$. Hence, the forgetful map $E_1 \to E_2$ is a 5-isogeny that carries all 5 rational cusps to the identity; i.e., its kernel is the constant $\mathbb{Q}$-group $\mathbb{Z}/5\mathbb{Z}$. Thus, the dual isogeny has kernel $\mu_5$.

But $E_2(\mathbb{Q})$ is also finite with order 5, consisting of the points

$$\{(5,5)(5,-6), (16,60), (16,-61), \infty\},$$

so the quotient of $E_2$ by that $\mathbb{Q}$-subgroup $\mathbb{Z}/5\mathbb{Z}$ is not $E_1$ (as otherwise composing these would yield an endomorphism of $E_1$ of degree 25, necessarily with kernel $E_2[5]$ since $E_2$ has non-integral $j$-invariant and hence is not CM, so then $E_1[5]$ would be an extension of $\mathbb{Z}/5\mathbb{Z}$ by $\mathbb{Z}/5\mathbb{Z}$ as a $\mathbb{Q}$-group; the $\mu_5$-valued Weil pairing on $E_1[5]$ would then give a contradiction). This quotient of $E_2$ must then be another elliptic curve over $\mathbb{Q}$, so it is $E_3$.

To summarize, we have 5-isogenies

$$E_1 \to E_2 \to E_3.$$

By design, each has kernel $\mathbb{Z}/5\mathbb{Z}$ as a $\mathbb{Q}$-group. Since the $L$-function is invariant under isogeny, we have

$$L(1, E_1) = L(1, E_2) = L(1, E_3) \approx 0.2538 \ldots.$$

Therefore, the BSD conjecture predicts that the quantity on the right side of (1.1) is also the same for $E_1, E_2$, and $E_3$. In all three cases $\text{III} = 0$. The regulator $R_E$ is also trivial since the common rank of these $\mathbb{Q}$-isogenous curves is 0. However, the volume and Tamagawa factors vary, as follows.
1. The common Galois module \( E_i[2] \) is not split over \( \mathbb{R} \) (the cubic \( 4x^3 - 4x^2 + 1 \) for \( E_1 \) has negative discriminant \(-44\) and so has one real root), so the 1-dimensional compact commutative Lie groups \( E_i(\mathbb{R}) \) are all connected and hence are circles. Since the Weierstrass models described above are minimal, and the smooth part of the minimal Weierstrass model coincides with the relative identity component of the Néron model, a Néron differential on each \( E_i \) is given by \( dx/(2y+1) \). Hence, for \( E_1 \) the volume term is

\[
\Omega_1 =: \Omega_{E_1} = \int_{E(\mathbb{R})} \left| \frac{dx}{2y+1} \right| = 2 \int_{\alpha}^{\infty} \frac{dx}{\sqrt{4x^3 - 4x^2 + 1}}
\]

where \( \alpha \) is a real root of \( 4x^3 - 4x^2 - 1 \).

This volume turns out to be \( 25L(1, E) \), expressing that \( \#E_1(\mathbb{Q}) = 5 \), and \( c_p = 1 \) for all \( p \). The triviality of \( c_p \) for \( p \neq 11 \) is clear by the moduli-theoretic meaning of \( E_1 \) (or by hand: good reduction away from 11), and for \( p = 11 \) we note that \( E_1 \) has split multiplicative reduction. Consequently, by the theory of Tate curves and the link between the minimal regular proper model and the Néron model for an elliptic curve (the latter being the smooth part of the former) it follows that \( c_{11} = -v_{11}(j) = -1 \).

It is a general theorem that the Jacobian of \( X_1(\ell) \) has Néron model with connected fiber at \( \ell \) for all primes \( \ell > 3 \), but this requires computing the minimal regular proper model of \( X_1(\ell) \) over \( \mathbb{Z}(\ell) \), which is much harder than for \( X_0(\ell) \) and is also harder in general than for the genus-1 case \( \ell = 11 \).

2. For \( E_2 \), we have \( \Omega_2 = \Omega_1/5 \). The other factors must change to compensate, and it turns out that the change is \( c_{11} = 5 \). This comes from the fact that \( v_{11}(j(E_2)) = -5 \) and \( E_2 \) has split multiplicative reduction (since \( E_1 \) has that property); in contrast, a quadratic twist \( E'_2 \) of \( E_2 \) by a character that is unramified but nontrivial locally at 11 would have \( c'_{11} = 1 \) even though \( v_{11}(j') = -5 \) too.

3. For \( E_3 \), we have \( \Omega_3 = \Omega_2/5 \). Here the changes relative to \( E_2 \) are that \( c_{11} = 1 \) (because the reduction type is split multiplicative and \( v_{11}(j) = -1 \)) but \( E_3(\mathbb{Q}) = 0 \).

We have seen that the variation in the \( j \)-invariants, coupled with the theory of Tate curves and minimal regular proper models, explains the variation of the Tamagawa factors. Let’s explain why the volume terms are changing.

In all three cases, we have seen that \( E_i(\mathbb{R}) \) is a circle. The induced maps \( E_i(\mathbb{R}) \to E_{i+1}(\mathbb{R}) \) are therefore finite-degree homomorphisms from the circle onto itself as a Lie group, of degree equal to the size of the kernel. But we rigged both isogenies over \( \mathbb{Q} \) to have kernel \( \mathbb{Z}/5\mathbb{Z} \), so on \( \mathbb{R} \)-points the kernel has order 5; i.e., it is a degree-5 map between Lie groups. Hence, the effect on periods is precisely division.
by 5 (from the degree of the map) provided that a Néron differential pulls back to a Néron differential under each map \( N(E_i) \to N(E_{i+1}) \). In other words, we have to prove that this \( \mathbb{Z} \)-homomorphism between smooth \( \mathbb{Z} \)-groups is étale.

Over \( \mathbb{Z}[1/11] \) the map \( N(E_i) \to N(E_{i+1}) \) between abelian schemes must be finite flat, and its generic fiber is a constant \( \mathbb{Q} \)-group of order 5 by design. But away from 5 this kernel must then be finite étale, hence the same constant group. By Raynaud’s work on finite flat group schemes, the kernel must be constant over \( \mathbb{Z}(5) \) as well (or more concretely, the points in the kernel are clearly distinct modulo 5 for each isogeny), so overall we have the étaleness away from 11. It remains to study the situation at 11.

If you look at the points in \( E_2(\mathbb{Q}) \) aside from the identity, they all have the same reduction at 11, namely \((5,5)\). This is the singularity in the mod-11 fiber of the minimal Weierstrass model, so over \( \mathbb{Z}(11) \) these points have reduction in the Néron model that lie in non-identity components of the mod-11 fiber. Consequently, we see that the quasi-finite flat schematic closure in \( N(E_2) \) of the kernel of \( E_2 \to E_3 \) has mod-11 fiber that is also a constant group consisting of 5 distinct points. Since \( N(E_2)_{\mathbb{F}_{11}} \) has 5 connected components and \( N(E_3)_{\mathbb{F}_{11}} \) is connected, we conclude that \( N(E_2) \to N(E_3) \) is actually surjective even on mod-11 fibers and its kernel is the constant group \( \mathbb{Z}/5\mathbb{Z} \) over \( \mathbb{Z} \). Hence, this map between Néron models is the quotient by that constant group, and in particular it is an étale morphism as desired.

### 1.1 Computing \( X \)

Finally, let’s discuss computing \( X \), focusing on \( \text{III}(E)[2] \) for \( E \) one of the curves discussed above. This is a subgroup of \( H^1(G_{\mathbb{Q},S}, E[2]) \), where \( S = \{2, 11\} \) (the ramified places for \( E[2] \)). We will compute this ambient degree-1 cohomology group, and find that it is 2-dimensional over \( \mathbb{F}_2 \) (and then when further local conditions are imposed to get \( \text{III}(E)[2] \) one gets 0). Since 5-isogenies induce isomorphisms on 2-torsion, the problem is literally the same for each \( E \).

Abstractly \( M := \text{E}[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2 \simeq \{(u, v, w) \in (\mathbb{Z}/2\mathbb{Z})^3 : u + v + w = 0\} \) on which the Galois action is given by a map \( G_S \to S_3 \) corresponding to the cubic equation defining \( \text{E}[2] \). This is the standard permutation representation, and the splitting field of \( \text{E}[2] \) is an \( S_3 \)-extension of \( \mathbb{Q} \).

**Remark 1.2.** Tate’s global Euler characteristic for Galois cohomology (as will be discussed in Jeremy’s talk) says

\[
\frac{\#H^1(G_S, M)}{\#H^0(G_S, M) \cdot \#H^2(G_S, M)} = \frac{\#M}{\#M^{\text{Gal}(\mathbb{C}/\mathbb{R})}}.
\]

Since our cubic has only one real root, we have \( \#M^{\text{Gal}(\mathbb{C}/\mathbb{R})} = 2 \). Also, \( \#M = \#E[2] = 4 \). We also know \( \#H^0(G_S, M) = 1 \) because \( E(\mathbb{Q}) \) has no non-trivial 2-torsion points, so \( \#H^1(G_S, M)/\#H^2(G_S, M) = 2 \). We’ll show \( \#H^1(G_S, M) = 4 \) (so \( \#H^2(G_S, M) = 2 \)).
There is only one way to approach the $H^1$-computation, which is to pass to the splitting field (which lies inside $\mathbb{Q}_S$). Let $K$ be the cubic extension of $\mathbb{Q}$ obtained by adjoining a root $\alpha$ of $4x^3 - 4x + 1$, and $L$ its Galois closure, so $L$ has a unique quadratic extension $\mathbb{Q}(\sqrt{-11})$.

Obviously $\text{Gal}(\mathbb{Q}_S/L)$ acts trivially on $E[2]$. There is a spectral sequence

$$H^p(G_L/\mathbb{Q}, H^q(\mathbb{Q}_S/L, M)) \Rightarrow H^{p+q}(G_{\mathbb{Q}_S}, M)$$

whose $E_2$ page is

$$H^0(G_L/\mathbb{Q}, H^2(\mathbb{Q}_S/L, E[2])) \quad \ldots$$

$$H^0(G_L/\mathbb{Q}, H^1(\mathbb{Q}_S/L, E[2])) \quad H^1(G_L/\mathbb{Q}, H^1(\mathbb{Q}_S/L, E[2])) \quad \ldots$$

$$H^0(G_L/\mathbb{Q}, H^0(\mathbb{Q}_S/L, E[2])) \quad H^1(G_L/\mathbb{Q}, H^0(\mathbb{Q}_S/L, E[2])) \quad \ldots$$

It turns out that everything beyond the left column vanishes, but this is not obvious, so the spectral sequence degenerates at this page. The reason is that on a $p$-torsion module Galois cohomology injects into that of a $p$-Sylow subgroup, and $E[2]$ happens to be a free module over the group algebra on a 2-Sylow of this $S_3$.

Therefore, what we want is

$$H^1(\mathbb{Q}_S/L, E[2])^{G_L/\mathbb{Q}} = (E[2] \otimes H^1(\mathbb{Q}_S/L, \mathbb{Z}/2\mathbb{Z}))^{G_L/\mathbb{Q} \simeq S_3}.$$
general if $G$ is a finite group and $V$ is a $k[G]$-module for a ring $k$ then we claim that $k[G] \otimes_k V$ is an induced module (so has vanishing higher cohomology); this is due to the classical observation that for the underlying $k$-module $V_0$ with trivial action we have a $G$-module isomorphism $k[G] \otimes_k V \simeq k[G] \otimes_k V_0$ via $g \otimes v \mapsto g \otimes (g.v)$.

The upshot is that to compute the size of $(U \otimes H^1(Q_S/L,\mathbb{Z}/2\mathbb{Z}))^{S_3}$, it suffices to find a filtration of $H^1(Q_S/L,\mathbb{Z}/2\mathbb{Z})$ as an $S_3$-module and compute the sizes for $S_3$-invariants of $U$ tensored against each successive quotient in the filtration.

The ring $O_{L,S}$ of $S$-integers of $L$ has trivial class group, so the $S$-integral Kummer sequence gives

$$H^1(Q_S/L,\mathbb{Z}/2\mathbb{Z}) = H^1(Q_S/L,\mu_2) = O_{L,S}/(O_{L,S})^2$$

as a $G_{L/Q}$-module. The unit group is

$$O_{L,S}^\times = \langle \pi_2, \pi_{11}^0, \pi_{11}^b, \pi_{11}^c \rangle O_L^\times,$$

where $\pi_{11}^{a,b,c}$ are respective generators for the three primes lying over 11 (and $\pi_2$ is a generator for the unique prime over 2). Thus, we have an exact sequence of $G_{L/Q}$-modules

$$1 \to O_L^\times/(O_L^\times)^2 \to O_{L,S}^\times/(O_{L,S}^\times)^2 \to T \oplus T \oplus U \to 0.$$

Tensoring against $U$ and taking invariants, the right term gives

$$(U \otimes U \otimes (U \otimes U))^{S_3} = (U \otimes U)^{S_3} = (U^* \otimes U)^{S_3} = \text{End}_{S_3}(U) = \mathbb{F}_2.$$

Thus, it remains to show that $(U \otimes (O_L^\times/(O_L^\times)^2))^{S_3}$ is 1-dimensional over $\mathbb{F}_2$. Consider the filtration

$$1 \to \langle -1 \rangle \to O_L^\times/(O_L^\times)^2 \to O_L^\times/(\langle -1 \rangle \cdot (O_L^\times)^2) \to 1.$$

The quotient $O_L^\times/(\langle -1 \rangle)$ is free of rank 2, and by computing a basis one sees by inspection that the action of $G_{L/Q}$ gives the standard representation of $S_3$ on $\mathbb{Z}^2$. Hence, $O_L^\times/(O_L^\times)^2$ is an extension of $U$ by $T$, so applying the exact functor $(U \otimes (\cdot))^{S_3}$ gives a further contribution of $(U \otimes U)^{S_3}$ that we have already seen is 1-dimensional. Hence, $H^1(G_{Q,S}, E[2])$ is 2-dimensional as claimed.