Kolyvagin's Theorem

Ravi Fernando – fernando@berkeley.edu

October 6, 2015*

1 Introduction and statement of results

In this talk, we'll discuss in more detail the result of Kolyvagin stated below, which implies the Birch and Swinnerton-Dyer conjecture for analytic rank 0 and 1. We won't prove the strong version of the statement, but we will essentially prove the weak version over the course of the next few talks.

Our general setup is as follows: E is an elliptic curve defined over $\mathbb{Q}$ with conductor N, so that there exists a modular parametrization $\phi : X_0(N) \to E$. Let K be the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ of discriminant $-D$, chosen so that every prime dividing N splits in K. (For simplicity, we'll assume that $D \neq 3$ or 4, so that we don't have extra units in $\mathcal{O}_K$.) Then choosing a squarefree integer n relatively prime to N and D (as well as the prime p that we'll introduce soon) yields the Heegner points $x_n = (\mathcal{C}/\mathcal{O}, \mathfrak{N}_n^{-1}/\mathcal{O}) \in X_0(N)$, which we can transport to $y_n \in E$. These points are defined over the ring class field K_n of conductor n. In particular, y_1 is defined over the Hilbert class field K_1, and its trace $y_K = \mathrm{Tr}_{K_1/K}(y_1)$ (defined using the group law of E) is defined over K.

Kolyvagin's main theorem is as follows.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve, and assume that y_K is non-torsion in $E(K)$. Then $E(K)$ has rank 1 and $Ш(E/K)$ is finite.*

Notice that the Gross-Zagier formula relates this to BSD: by Gross-Zagier, we have y_K non-torsion $\iff h_E(y_K) \neq 0 \iff L'(1, E/K) \neq 0$.

This is hard (and isn't proved in most references), so we'll spend the next few weeks proving a weaker version:

Theorem 1.2. *Let p be an odd prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$, and assume that p does not divide y_K in $E(K)/E(K)_{\mathrm{tors}}$. Then $E(K)$ has rank 1 and $Ш(E/K)$ has trivial p-torsion.*

*Notes for a talk given in Berkeley's Student Heegner Point Seminar, supervised by Xinyi Yuan. Main reference: Francesca Gala's master's thesis, *Heegner points on $X_0(N)$*.

The following is a somewhat more accessible statement that we will use to prove the above:

Proposition 1.3. *Let p be an odd prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$, and assume that p doesn't divide y_K in $E(K)/E(K)_{\mathrm{tors}}$. Then $\mathrm{Sel}_p(E/K)$ is cyclic, generated by $\delta(y_K)$.*

Let's see why 1.3 implies 1.2. Recall the short exact sequence of $\mathbb{F}_p$-vector spaces

$$0 \to E(K)/pE(K) \xrightarrow{\delta} \mathrm{Sel}_p(E/K) \to \text{Ш}(E/K)[p] \to 0. \tag{1}$$

If 1.3 holds, then δ is both injective and surjective, so $\text{Ш}(E/K)[p]$ is trivial. It also follows that $E(K)/pE(K)$ has dimension 1 over $\mathbb{F}_p$, so $E(K)$ has rank at most 1. But the rank is also at least 1, because y_K is a non-torsion point by hypothesis.

We'll spend the next few talks proving 1.3. The high-level outline will be as follows:

1. Study the action of $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ on the p-torsion of E, and look at Kolyvagin primes.
2. Show that the Heegner points $y_n \in E(K_n)$ form an Euler system.
3. Construct a system of interesting cohomology classes $c(n) \in H^1(K, E[p]) = H^1(G_K, E(\overline{K})[p])$.
4. Study the properties of $c(n)$, including their behavior under complex conjugation and their triviality in $H^1(K_v, E[p])$.
5. Use facts from Galois cohomology theory (Tate local duality) to bound the order of $\mathrm{Sel}_p(E/K)$ and complete the proof.

This talk will focus on items 1 and 2 above, as well as Serre's open image theorem, which will help us understand the hypothesis that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ and why it makes sense to assume it.

2 Galois action on torsion points

2.1 Serre's open image theorem

For E an elliptic curve defined over a number field K, the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on (the $\overline{K}$-points of) E by acting on coordinates, and as a result it acts on the n-torsion points of E for each n. Recall that for ℓ prime, the ℓ-adic Tate module $T_\ell(E)$ is defined to be the inverse limit $\lim_{\infty \leftarrow n} E[\ell^n]$. Since $E[\ell^n]$ is always a rank-2 free module over $\mathbb{Z}/\ell^n\mathbb{Z}$, it follows that $T_\ell(E)$ is a rank-2 free $\mathbb{Z}_\ell$-module, and that $\lim_{\infty \leftarrow n} E[n] = \bigoplus_\ell T_\ell E$ is a rank-2 free module over $\bigoplus_\ell \mathbb{Z}_\ell = \widehat{\mathbb{Z}}$. Consequently, the action of G_K on E yields a representation $\rho_E : G_K \to \mathrm{Aut}(\lim_{\infty \leftarrow n} E[n]) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Of course, since $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, we can focus on a single prime if we like, and consider $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$, or even reduce mod the maximal ideal to obtain $\overline{\rho}_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$.

Serre's open image theorem tells us that if E doesn't have complex multiplication, then the total Galois representation $\rho_E : G_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ has an open image, when $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is given the profinite topology. In particular, since $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is profinite, this implies that $\rho_E(G_K)$ has finite index in it. An equivalent statement[1] is that (1) $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ has open image for all ℓ, and (2) it is surjective for almost all ℓ.

To connect this to the hypotheses of Theorem 1.2 (with $K = \mathbb{Q}$), notice that the open image theorem implies that $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) = \mathrm{GL}_2(\mathbb{F}_p)$ is surjective for almost all p. In particular, $G_{\mathbb{Q}}/\ker \overline{\rho}_{E,p}$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. But $\ker \overline{\rho}_{E,p}$ is the subgroup of $G_{\mathbb{Q}}$ preserving the coordinates of all the p-torsion points of E, so $G_{\mathbb{Q}}/\ker \overline{\rho}_{E,p}$ is just $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. Thus it is reasonable to assume that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ for our particular p, since (if E doesn't have complex multiplication) this is necessarily true for all but finitely many p.

2.2 Action of $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ on p-torsion

Proposition 2.1. *The extension $K(E[p])/K$ is unramified away from pN.*

Proof. Let λ be a prime of K not above pN, and let γ be a prime of $K(E[p])$ lying over λ. Since $\lambda \nmid N$, E has good reduction over $\mathcal{O}_{K_\lambda}$. There is a theorem that in the case of good reduction, the prime-to-ℓ torsion of E over $\mathcal{O}_{K_\lambda}$ injects into that of the reduction $\widetilde{E}$ over $\mathbb{F}_\lambda$. Now we can view an element g of the inertia group as an automorphism of $K(E[p])_\gamma/K_\lambda$ fixing the residue field $\mathbb{F}_\gamma/\mathbb{F}_\lambda$. But if g fixes $\mathbb{F}_\gamma$, then it fixes $\widetilde{E}(\mathbb{F}_\gamma)$, so it fixes $E[p]$ and therefore is trivial. It follows that $I_{\gamma/\lambda}$ is trivial, so the extension is unramified over λ. ☐

Definition 2.2. *Let* Frob_ℓ *denote the conjugacy class in* $\mathrm{Gal}(K(E[p])/\mathbb{Q})$ *containing the Frobenius elements for* $\mathrm{Gal}(\mathbb{F}_\gamma/\mathbb{F}_\ell)$ *for every γ over ℓ. We say that ℓ is a* Kolyvagin prime *if complex conjugation, τ, belongs to* Frob_ℓ.

Notice that the Chebotarev density theorem implies that there are infinitely many Kolyvagin primes. Also notice that if ℓ is a Kolyvagin prime, then $[\mathbb{F}_\gamma : \mathbb{F}_\ell] = 2$ for all primes $\gamma | \ell$; that is, the inertia degree is 2. From now on, we will always assume that ℓ is a Kolyvagin prime.

Proposition 2.3. *Let ℓ be a Kolyvagin prime, and define a_ℓ by $\ell + 1 - a_\ell = |\widetilde{E}(\mathbb{F}_\ell)|$. Then we have $a_\ell \equiv \ell + 1 \equiv 0 \pmod p$.*

Proof. If we let G_K act on $E[p]$, then complex conjugation has characteristic polynomial $x^2 - 1$, and any element of $\mathrm{Frob}(\ell)$ has characteristic polynomial $x^2 - a_\ell x + \ell$. (Recall what the Weil conjectures say about elliptic curves: the characteristic polynomial of $\mathrm{Frob}(\ell)$ on $E[p]$ is $(x - \alpha)(x - \overline{\alpha})$ where $|\alpha| = \sqrt{\ell}$, and $|E(\mathbb{F}_{\ell^n})| = \ell^n + 1 + \alpha^n + \overline{\alpha}^n$ for all n. Here, $a_\ell = \alpha + \overline{\alpha}$, and $\ell = \alpha\overline{\alpha}$.) If ℓ is a Kolyvagin prime, these are congruent mod p, so a_ℓ and $\ell + 1$ are both divisible by p. ☐

Proposition 2.4. *Let $\widetilde{E}(\mathbb{F}_\lambda)[p]^\pm$ be the $+1$ and -1 eigenspaces of complex conjugation acting on $\widetilde{E}(\mathbb{F}_\lambda)$. Then each is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and $\widetilde{E}(\mathbb{F}_\lambda)$ is their direct sum.*

Proof. Since $\widetilde{E}(\mathbb{F}_\lambda)[p]^+$ is just $\widetilde{E}(\mathbb{F}_\ell)$, its order is $\ell + 1 - a_\ell \equiv 0 \pmod p$. On the other hand, $\widetilde{E}(\mathbb{F}_\lambda)[p]^-$ is the kernel of $\tau + 1 = \mathrm{Fr}_\ell + 1$. This can be shown to be congruent to $\mathrm{Tr}(\mathrm{Fr}_\ell) + \det(\mathrm{Fr}_\ell) + 1 \equiv a_\ell + \ell + 1 \equiv 0 \bmod p$. ☐

[1]See the second page of Serre's paper, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", available online.

3 Euler systems

Historical anecdote: you may have heard of Euler systems before in the context of Wiles's first (incomplete) proof of Fermat's Last Theorem. The gap in the original proof, discovered by Nick Katz, was (to the best of my understanding) that Wiles asserted something was an Euler system, but it wasn't. This led to an incorrect bound on the order of a Selmer group, and ultimately Wiles and Taylor spent almost a year filling the gap. After today, you will not make this mistake.

Now we're going to look more carefully at the collection of Heegner points $y_n \in E(K_n)$, as n varies. Recall our standing assumptions: n is squarefree and coprime to NDp, and every $\ell | n$ is a Kolyvagin prime. For $\ell | n$, set $m = n/\ell$. Let G_n denote $\mathrm{Gal}(K_n/K_1)$. Some nice facts about ring class fields: K_ℓ and K_m are disjoint over K_1, giving us $G_\ell = \mathrm{Gal}(K_n/K_m)$ and $G_m = \mathrm{Gal}(K_n/K_\ell)$ and thus $G_n \cong G_\ell \times G_m$, and in fact $\cong \prod_{\ell|n} G_\ell$. We also have $G_n = (\mathcal{O}_K/n\mathcal{O}_K)^\times/(\mathbb{Z}/n\mathbb{Z})^\times$ in general, and in particular $G_\ell = \mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times$, which is cyclic of order $\ell + 1$.

We're now ready to state and prove the Euler system properties.

Definition and proposition 3.1. *A family of elements $y_n \in E(K_n)$, indexed by the integers n with the properties above, forms an* Euler system *if the following compatibility conditions hold:*

1. $\mathrm{Tr}_\ell\, y_n = a_\ell \cdot y_m \in E(K_m)$, *where Tr_ℓ denotes the sum of the G_ℓ-conjugates under the group law of E.*
2. *For each prime λ_n over ℓ in K_n, letting λ_m be the prime under it in K_m, we have $y_n \equiv \mathrm{Frob}(\lambda_m) y_m \pmod{\lambda_n}$.*

The Heegner points $y_n \in E(K_n)$ form an Euler system.

Proof. (Idea.) For (1), write y_n as $\phi(x_n)$, where $\phi : X_0(N) \to E$ is the modular parametrization, and use facts about the Hecke operators T_ℓ. For (2), do all your calculations on $X_0(N)$ instead of E, proving that $x_n \equiv \mathrm{Frob}(\lambda_m) x_m$ in $\mathbb{F}_{\lambda_n}$. □

Remark 3.2. *In general, an Euler system may be somewhat different from this. Often an Euler system consists of elements c_F of the Galois cohomology groups $H^1(F, T_\ell E)$ indexed by fields F containing a given number field K. Here, of course, we can view our x_n's as being indexed by the fields K_n instead of the integers n, but we're also looking at elements in $E(K_n) = H^0(K_n, E(\overline{K}))$ rather than $H^1(K_n, T_\ell E)$. So it seems that the notion of an Euler system is a fairly general one, and really just means a family of elements satisfying compatibility conditions similar to the ones above.*