Kolyvagin - BUNTES

Throughout this semester, we learned about the Gross and Zagier's theorem. Kolyvagin proved a theorem, which in conjunction with Gross and Zagier's theorem and an additional conjecture implies the for any modular elliptic curve E, if $L(E, 1) \neq 0$, then $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ are finite. We know this for elliptic curves with complex multiplication, as proven by Coates and Wiles for $E(\mathbb{Q})$ and Rubin for $Ш_{E/\mathbb{Q}}$.

1 Set up and Notation

Let E be an elliptic curve defined over $\mathbb{Q}$, and assume that E is modular, i.e. for some integer N, there is a nonconstant map $\pi : X_0(N) \to E$ defined over $\mathbb{Q}$.

We choose an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ which we fix.

We will following the notation below:

- K: fixed imaginary quadratic field in which all primes dividing N splits
- τ: complex conjugation of K
- $[\tau]$: conjugacy class of τ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $\mathfrak{a}$: ideal of K such that $\mathcal{O}_K/\mathfrak{a} \equiv \mathbb{Z}/N\mathbb{Z}$
- H: Hilbert class field of K
- x_H: point in $X_0(N)(\mathbb{C})$ corresponding to the pair $(\mathbb{C}/\mathcal{O}_K, \mathfrak{a}^{-1}/\mathcal{O}_K)$
- y_H: denotes $\pi(x_H) \in E(H)$
- y_K: denotes $\mathrm{Tr}_{H/K}(y_H) \in E(K)$
- y: denotes $y_K - y_K^\tau$
- $Ш_{E/\mathbb{Q}}$: Tate-Shafarevich group of E over $\mathbb{Q}$
- A_n: denotes the n-torsion points of an abelian group A
- A_{n^∞}: denotes the union $\bigcup_i A_{n^i}$
- $H^i(L/F, A)$: denotes $H^i(\mathrm{Gal}(L/F), A)$
- $H^i(F, A)$: $H^i(\overline{F}/F, A)$
- $H^i(F, E)$: $H^i(F, E(\overline{F}))$

Remark 1.1. CM theory tells us that $x_H \in X_0(N)(H)$, so we are justified in defining y_H.

2 Main theorems

Theorem 2.1 (Gross-Zagier)**.** *y has infinite order in $E(K)$ if and only if $L(E, 1) \neq 0$ and $L'(E, \chi_K, 1) \neq 0$, where χ_K is the quadratic character attached to K.*

Theorem 2.2 (Kolyvagin)**.** *If y has infinite order in $E(K)$ then $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ are finite.*

Conjecture 2.3 (Analytic Conjecture)**.** *If E is a modular elliptic curve and sign in the funbctional equation of $L(E, s)$ is $+1$, then there exists at least one imaginary quadratic field K, in which all primes dividing N split, such that $L'(E, \chi_K, 1) \neq 0$.*

Consequence 2.4. *For any modular elliptic curve E, if $L(E,1) \neq 0$, then $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ are finite.*

Remark 2.5. The consequence 2.4 is true for elliptic curves with CM. Coates and Wiles proved the finiteness of $E(\mathbb{Q})$ and Rubin proved the finiteness of $Ш_{E/\mathbb{Q}}$ for this case.

3 Preliminary Stuff

For a prime number p and a positive integer n, we can take any completion $\mathbb{Q}_v$ of $\mathbb{Q}$ to get the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/p^n E(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E_{p^n}) & \longrightarrow & H^1(\mathbb{Q}, E)_{p^n} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{res}_v & & \downarrow \mathrm{res}_v & & \\ 0 & \longrightarrow & E(\mathbb{Q}_v)/p^n E(\mathbb{Q}_v) & \longrightarrow & H^1(\mathbb{Q}_v, E_{p^n}) & \longrightarrow & H^1(\mathbb{Q}_v, E)_{p^n} & \longrightarrow & 0 \end{array}$$

The Selmer group $S^{(p^n)}$ and the p^n-torsion of the Tate-Shafarevich group, $Ш_{p^n}$ are defined as

$$S^{(p^n)} = \bigcap_v \mathrm{res}_v^{-1}(\text{image } E(\mathbb{Q}_v))$$

$$0 \to E(\mathbb{Q})/p^n E(\mathbb{Q}) \to S^{(p^n)} \to Ш_{p^n} \to 0.$$

We will show that $S^{(p)} = 0$ for almost all p. The remaining p will have $S^{(p^n)}$ of order annihilated by a power of p which will be independent of n.

Proposition 3.1. *Suppose ℓ is a prime such that $E(\mathbb{Q}_\ell)_{p^n} \equiv \mathbb{Z}/p^n\mathbb{Z}$, $k \geq 0$ is an integer, and $c_\ell \in H^1(\mathbb{Q}, E)_{p^n}$ satisfies*

(a) for all $v \neq \ell$, $\mathrm{res}_v(c_\ell) = 0$

(b) $\mathrm{res}_\ell(c_\ell)$ has order p^{n-k}

Then for every $s \in S^{(p^n)}$, $p^k \,\mathrm{res}_\ell(s) = 0$.

The existence of c_ℓ for sufficiently man ℓ with bounded k which is almost always 0 is given by Proposition 3.5.

We construct the element c_ℓ using Heegner points. Let ℓ be a rational prime that is inert in K and $\ell \nmid N$. Let $\mathcal{O}_\ell$ be the order of the conductor ℓ in $\mathcal{O}_K$ and x_ℓ be the point in $X_0(N)(\mathbb{C})$ corresponding to the pair $(\mathbb{C}/\mathcal{O}_\ell, (\mathfrak{a} \cap \mathcal{O}_\ell)^{-1}/\mathcal{O}_\ell)$. CM implies $x_\ell \in X_0(N)(K[\ell])$ where $K[\ell]$ is the class field corresponding to the subgroup $K^\times \mathbb{C}^\times \prod_q (\mathcal{O}_\ell \otimes \mathbb{Z}_q)^\times$ of the ideles of K.

Notice that $K[\ell]$ is a cyclic extension of H of degree $(\ell+1)/u_K$ where $u_K = \#(\mathcal{O}_K^\times)/2$. $K[\ell]$ is also totally ramified at ℓ and only ramified there. τ acts on $\mathrm{Gal}(K[\ell]/K)$ by -1. Let $y_\ell = \pi(x_\ell \in E(K[\ell])$. The following proposition contains the facts we need about Heegner points.

Proposition 3.2. *(a) $u_K \,\mathrm{Tr}_{K[\ell]/H}(y_\ell) = a_\ell y_H$*

(b) For any prime λ of $K[\ell]$ above ℓ, $\widetilde{y}_\ell = \widetilde{y}_H^{\mathrm{Frob}} \in \widetilde{E}(\mathbb{F}_{\ell^2})$ where $\sim$ denotes reduction modulo ℓ.

Proof. Let A be an elliptic curve defined over H with CM by $\mathcal{O}_K$ so that $(A, A_\mathfrak{a})$ represents x_H. WLOG, let A have good reduction at all primes above ℓ. Let $\mathcal{C}$ be the collection of $\ell+1$ subgroups of order ℓ of A. Notice that x_ℓ can be represented by $(A', A'_\mathfrak{a})$ where $A' = A/C_\ell$ where C_ℓ is a subgroup of order ℓ.

$\mathrm{Gal}(K[\ell]/H)$ acts transitively on $\mathcal{C}/\mathrm{Aut}(E)$ which has order $(\ell+1)/u_K = [K[\ell] : H]$. Thus, the Hecke correspondence on $X_0(N)$ can be written as

$$T_\ell(x_H) = \sum_{C\in\mathcal{C}} (A/C, (A/C)_{\mathfrak{a}}) = u_K \sum_{\sigma\in\mathrm{Gal}(K[\ell]/H)} (x_\ell)^\sigma.$$

Composing the above with π gives the first part of the proposition.

Now, consider the isogeny $\phi : (A, A_{\mathfrak{a}}) \to (A', A'_{\mathfrak{a}})$. Since ℓ is inert, A and A' have supersingular reduction at λ. Thus, the reduced isogeny $\widetilde{\phi} : (\widetilde{A}, \widetilde{A}_{\mathfrak{a}}) \to (\widetilde{A}', \widetilde{A}'_{\mathfrak{a}})$ must be Frobenius up to automorphism. Thus, $\widetilde{x}_p = \widetilde{x}_H^{\mathrm{Frob}}$ in $\widetilde{X}_0(N)(\mathbb{F}_{\ell^2})$. By the universal property of the Neron model, π reduces to a morphism $\widetilde{\pi} : \widetilde{X}_0(N) \to \widetilde{E}$. Applying this $\widetilde{\pi}$ gives the second part of the proof. ☐

Lemma 3.3. *Suppose ℓ is a prime not dividing pD_KN, $r > 0$, and $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbb{Q}) = [\tau]$. Then if $\widetilde{E}$ is the reduction of E modulo ℓ and $a_\ell = \ell + 1 - \#(\widetilde{E}(\mathbb{F}_\ell))$, we get*

(a) $p^r \mid a_\ell$ *and* $p^r \mid \ell + 1$

(b) *ℓ remains prime in K*

(c) $E(\mathbb{Q}_\ell)_{p^r} \equiv \widetilde{E}(\mathbb{F}_\ell)_{p^r} \equiv \mathbb{Z}/p^r\mathbb{Z}$

(d) $(E(K_\ell)_{p^r})^- \equiv (\widetilde{E}(\mathbb{F}_{\ell^2})_{p^r})^- \equiv \mathbb{Z}/p^r\mathbb{Z}$.

If ℓ is a prime not dividing pD_KN, $r > 0$ and $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbb{Q}) = [\tau]$, then by Lemma 3.3, $p^r \mid a_\ell$ and $p^r \mid u_K[K[\ell] : H]$, so by cyclicity, there is a unique subextension H' of $K[\ell]$ of degree p^r. Let ϕ be a choice of lift of $\mathrm{Frob}_\ell(H/\mathbb{Q})$ to $\mathrm{Gal}(H'/\mathbb{Q})$ and define $z_1 \in E(H')$ as the point

$$z_1 = u_K \,\mathrm{Tr}_{K[\ell]/H'}(y_\ell + y_\ell^\phi) - (a_\ell/p^r)(y_H + y_H^\phi).$$

Then we get the following immediate corollary of Proposition 3.2.

Corollary 3.4. *Suppose $\ell \nmid pD_KN$ and $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbb{Q}) = [\tau]$. Then, we have*

(a) $\mathrm{Tr}_{H'/H}(z_1) = 0$

(b) *For any $\sigma \in \mathrm{Gal}(H/K)$, let $\overline{\sigma}$ denote any lift of σ to $\mathrm{Gal}(H'/K)$. Then, modulo any prime λ above ℓ, we have*

$$\sum_{\sigma\in\mathrm{Gal}(H/K)} \widetilde{z_1^{\overline{\sigma}}} = -((\ell + 1 + a_\ell)/p^r)\widetilde{y}.$$

For each place v of $\mathbb{Q}$, define

$$m_v = \#(H^1(\mathbb{Q}_v^{\mathrm{unr}}/\mathbb{Q}_v, E(\mathbb{Q}_v^{\mathrm{unr}})))$$

which is finite (ref: Milne, Arithmetic duality theorems I.3.8). Furthermore, it is nontrivial at a finite number of places, so we can define

$$m(p) = \sup\{\mathrm{ord}_p(m_v)\}_v.$$

This number is then 0 for all but a finite number of primes p.

We now have the tools necessary to construct c_ℓ.

Proposition 3.5. *Suppose $\ell \nmid pD_KN$ and $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbb{Q}) = [\tau]$, where $r = n + m(p)$. Then there exists $c_\ell \in H^1(\mathbb{Q}, E)_{p^n}$ such that*

(a) $\mathrm{res}_v(c_\ell) = 0$ *for all* $v \neq \ell$

(b) *the order of* $\mathrm{res}_\ell(c_\ell)$ *in* $H^1(\mathbb{Q}_\ell, E)_{p^n}$ *is equal to the order of* y *in* $E(K_\ell)/p^nE(K_\ell)$.

Proof. First, assume $p \nmid [H : K]$. Then there is a unique extension K' of K of degree p^r in $K[\ell]$. Let

$$z = \mathrm{Tr}_{H'/K'}(z_1) \in E(K').$$

By Corollary 3.4, $\mathrm{Tr}_{K'/K}(z) = 0$. Let σ be a fixed generator of $\mathrm{Gal}(K'/K)$. This gives rise to a group isomorphism

$$\mathrm{Ker}(\mathrm{Tr}_{K'/K} : E(K') \to E(K))/(\sigma - 1)E(K') \equiv H^1(K'/K, E(K')).$$

Let $c'_\ell \in H^1(K'/K, E(K')) \subset H^1(K'/K, E(K'))$ be the image of z under this isomorphism.

The isomorphism is not τ-equivariant. However, τ does commute with $\mathrm{Tr}_{K[\ell]/K'}$, so we can conclude that $z^\tau = -z$. τ also acts by -1 on $\mathrm{Gal}(K'/K)$, so we can conclude that $(c'_\ell)^\tau = c'_\ell$, which means $c'_\ell \in (H^1(K, E)_{p^r})^+$.

Recall that for $p > 2$, the restriction map gives an isomorphism $H^1(\mathbb{Q}, E)_{p^r} \equiv (H^1(K, E)_{p^r})^+$. Thus, we can finally define

$$c_\ell = p^{m(p)} c'_\ell \in H^1(\mathbb{Q}, E)_{p^n}.$$

(If $p \mid [H : K]$, we do not necessarily have the field K', but we can use z_1 to define $c'_{1,\ell} \in H^1(H, E)_{p^r}$. c'_ℓ is defined to be the corestriction of $c'_{1,\ell}$ to $H^1(K, E)$. We can proceed with this construction, but with adjustments.)

If $v \neq \ell$, K'/K is unramified at v, so we have

$$\mathrm{res}_v(c_\ell) = p^{m(p)} \mathrm{res}_v(c'_\ell) \in p^{m(p)} H^1(\mathbb{Q}_v^{\mathrm{unr}}/\mathbb{Q}_v, E(\mathbb{Q}_v^{\mathrm{unr}}))_{p^r} = 0.$$

This is true by our definition of $m(p)$.

To determine the order of $\mathrm{res}_\ell(c_\ell)$ in $H^1(\mathbb{Q}_\ell, E)_{p^n}$, let I_ℓ be the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell, \mathbb{Q}_\ell)$, and consider the maps (which do not form an exact sequence)

$$H^1(\mathbb{Q} - \ell, E)_{p^n} \hookrightarrow H^1(I_\ell, E(\overline{\mathbb{Q}}_\ell))_{p^n} \xrightarrow{\sim} H^1(I_\ell, \widetilde{E}(\overline{\mathbb{F}}_\ell))_{p^n} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(K'/K), \widetilde{E}_{p^n}).$$

The first map is injective since E has good reduction at ℓ which makes $H^1(\mathbb{Q}_\ell^{\mathrm{unr}}/\mathbb{Q}_\ell, E(\mathbb{Q}_\ell^{\mathrm{unr}}))_{p^n}$ zero.

The second map is an isomorphism since the kernel of good reduction modulo ℓ is a pro-ℓ group.

The third map is an isomorphism since I_ℓ acts trivially on $\widetilde{E}(\overline{\mathbb{F}}_\ell)$ and $K'\mathbb{Q}_\ell^{\mathrm{unr}}$ is the unique abelian extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$ of exponent p^r.

The composition of these maps sends c_ℓ to the homomorphism which sends our generator σ of $\mathrm{Gal}(K'/K)$ to $p^{m(p)}\widetilde{z}$. Thus, the order of $\mathrm{res}_\ell(c_\ell)$ in $H^1(\mathbb{Q}_\ell, E)_{p^n}$ is the same order of $p^{m(p)}\widetilde{z}$ in $\widetilde{E}(\mathbb{F}_{\ell^2})$.

Corollary 3.4 shows $p^{m(p)}\widetilde{z} = -((\ell + 1 + a_\ell)/p^n)\widetilde{y}$. Up to a factor of 2, we have

$$\#(\widetilde{E}(\mathbb{F}_{\ell^2})^-) = \#(\widetilde{E}(\mathbb{F}_{\ell^2}))/\#(\widetilde{E}(\mathbb{F}_\ell)) = \ell + 1 + a_\ell.$$

Since $(\widetilde{E}(\mathbb{F}_{\ell^2})_{p^\infty})^-$ is cyclic by Lemma 3.3, we get that $(\ell + 1 + a_\ell)/p^n$ defines an isomorphism between $\widetilde{E}(\mathbb{F}_{\ell^2})^-/p^n\widetilde{E}(\mathbb{F}_{\ell^2})^-$ and $(\widetilde{E}(\mathbb{F}_{\ell^2})_{p^n})^-$. Thus, the order of $p^{m(p)}\widetilde{z}$ in $\widetilde{E}(\mathbb{F}_{\ell^2})$ is the same as the order of y in $E(K_\ell)/p^nE(K_\ell) \equiv \widetilde{E}(\mathbb{F}_{\ell^2})/p^n\widetilde{E}(\mathbb{F}_{\ell^2})$. □

Combining Proposition 3.1 and Proposition 3.5 gives the following corollary.

Corollary 3.6. *Suppose $\ell \nmid pD_KN$ and $\mathrm{Frob}_\ell(K(E_{p^{n+m(p)}})/\mathbb{Q}) = [\tau]$. If $k \geq 0$ and $p^{n-k-1}y \notin p^nE(K_\ell)$, then for all $s \in S^{(p^n)}$, $p^k s_\ell = 0$.*

Let $t \in H^1(K, E_{p^n})$ and write $\widehat{t}$ for the image of t under the restriction map

$$H^1(K, E_{p^n}) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K(E_{p^{n+m(p)}})), E_{p^n})^{\mathrm{Gal}(D(E_{p^{n+m(p)}})/K)}.$$

Lemma 3.7. *Suppose $t \in H^1(K, E_{p^n})^{\pm}$ and the image of $\widehat{t}$ is cyclic. Then the order of t is at most p^{a+b}, where p^a is theorder of the largest $\mathbb{Q}$-rational cyclic subgroup of E_{p^∞} and p^b is the exponent of $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n})$.*

Proof. Since $\widehat{t}$ is $\mathrm{Gal}(K(E_{p^{n+m(p)}}), K)$ equivariant, its image is $\mathrm{Gal}(\overline{K}/K)$-invariant. Since τ acts on $\widehat{t}$ by ± 1, the image is in fact rational over $\mathbb{Q}$. Thus if the image is cyclic, the order of $\widehat{t}$ is at most p^a. The kernel of the restriction map above is $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n})$, so t has order at most p^{a+b}. □

4 Proof of Kolyvagin

Fix a prime p not dividing $\#(\mathcal{O}_K^\times)$ and suppose y has infinite order in $E(K)$. Let $k = k(p)$ be the largest integer such that $y \in p^k E(K) + E(K)_{\mathrm{tors}}$. Fix some $n \geq k+1$.

First, assume the following:

(a) E has no p-isogeny defined over $\mathbb{Q}$

(b) $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n}) = 0$.

Both of these assumptions hold for all but a finite number of p by Serre's theorem (alternatively via the theory of CM).

Proposition 4.1. *Given assumptions (a) and (b), $p^k S^{(p^n)} = 0$.*

Let $r = n + m(p)$ and fix $s \in S^{(p^n)}$. Let $\widehat{s}$ be the restriction of s to $\mathrm{Gal}(\overline{Q}/K(E_{p^r}))$ and $\widehat{y}$ be the restriction of the image of y under the injection

$$E(K)^-/p^n E(K)^- \to H^1(K, E_{p^n}).$$

Let F be a fixed finite extension of $K(E_{p^r})$ which is Galois over $\mathbb{Q}$ such that both $\widehat{s}$ and $\widehat{y}$ factor through $G = \mathrm{Gal}(F/K(E_{p^r})$.

Choose any $\gamma \in G$ and a prime ℓ not dividing $pD_K N$ such that $\mathrm{Frob}_\ell(F/\mathbb{Q}) = [\gamma\tau]$. It follows that $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbb{Q}) = [\tau]$, and $\mathrm{Frob}_\ell(F/K(E_{p^r})) \in [(\gamma\tau)^2]$ so that

$$p^k s_\ell = 0 \Leftrightarrow p^k \widehat{s}((\gamma\tau)^2)$$
$$p^{n-k-1} y \in p^n E(K_\ell) \Leftrightarrow p^{n-k-1}\widehat{y}((\gamma\tau)^2) = 0$$

Since $\widehat{s}^\tau = \widehat{s}$, and $\widehat{y}^\tau = -\widehat{y}$,

$$\begin{aligned} \widehat{s}((\gamma\tau)^2) &= \widehat{s}(\gamma) + \widehat{s}(\tau\gamma\tau) \\ &= (1+\tau)\widehat{s}(\gamma) \\ \widehat{y}((\gamma\tau)^2) &= \widehat{y}(\gamma) + \widehat{y}(\tau\gamma\tau) \\ &= (1-\tau)\widehat{y}(\gamma). \end{aligned}$$

By Corollary 6, we conclude that for every $\gamma \in G$, either $p^k\widehat{s}(\gamma) \in (E_{p^n})^-$ or $p^{n-k-1}\widehat{y}(\gamma) \in (E_{p^n})^+$. Thus, we have

$$G = (p^k\widehat{s})^{-1}((E_{p^n}^-)) \cup (p^{n-k-1}\widehat{y}^{-1})((E_{p^n})^+).$$

If A and B are subgroups, then $A \cup B = A$ or $A \cup B = B$. Thus, we have $p^k\widehat{s}(G) \subset (E_{p^n})^-$ or $p^{n-k-1}\widehat{y}(G) \subset (E_{p^n})^+$.

By assumptions (1) and (2) in conjunction with Lemma 3.7, either $p^k s = 0 \in S^{(p^n)}$ or $p^{n-k-1} y = 0 \in E(K)/p^n E(K)$. By our definition of k, the latter is not possible, so $p^k S^{(p^n)} = 0$.

Since $k \neq 0$ for almost all p, this proves Kolyvagin's theorem (Theorem 2.2) except for the finite number of p-parts which have been ruled out.

Without the assumptions (1) and (2), Lemma 3.7 would give a weaker annihilator of $S^{(p^n)}$, but one that is still independent of n. This is done by using the theorem of Serre or the theory of CM to show that the exponent of $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n})$ is bound independent of n.

"With a little more care" (what a flex), one obtains a suitable annihilator when $p \mid \#(\mathcal{O}_K^\times)$, thereby completing the proof.