Gross–Zagier reading seminar

Lecture 9 • Brandon Carter • November 11, 2014

1. Introduction

We begin with the same setup as before: Let x be a Heegner point on $X_0(N)$, let c be the divisor $(x)-(\infty)$, and let d be the divisor $(x)-(0)$. We need to compute the Néron height pairing $\langle c, T_m c^\sigma \rangle = \langle c, T_m d^\sigma \rangle$. We have seen that this global height pairing decomposes into a sum of local height pairings. Andrew computed the local height pairings at the archimedean places two weeks ago; our goal will be to use the theory of canonical lifts to start the case where p is a split prime in K.

2. Reduction of CM elliptic curves

Throughout the section we let E denote a CM elliptic curve with $\mathrm{End}(E) = \mathcal{O}_K$, where $\mathcal{O}_K$ is the full ring of integers of K. Every result we will introduce does admit some generalization to elliptics curve with CM by a non-maximal order $\mathcal{O}$, but [**?**] only considers CM curves of the first type, so this will suffice for our purposes.

Recall that an elliptic curve E over a field k of characteristic p is called *ordinary* if $E[p](\overline{k}) \simeq \mathbb{Z}/p\mathbb{Z}$ and *supersingular* if $E[p](\overline{k}) = 0$. There are several equivalent definitions of a supersingular elliptic curve.

Theorem 1 ([**?**, Thm V.3.1])**.** *The following are equivalent:*
(a) $E[p](\overline{k}) = 0$.
(b) V *is inseparable.*
(c) $[p] : E \to E$ *is purely inseparable and* $j(E) \in \mathbb{F}_{p^2}$.
(d) $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

We will be considering the reduction of Heegner points to compute the local height pairings, and knowledge of the behavior of the reduction of CM elliptic curves will prove useful. Fortunately, the type of reduction at a place $v \mid p$ is determined by the splitting behavior of p in K.

Proposition 2. *Let E be an elliptic curve over a number field F with CM by K (i.e.* $\mathrm{End}(E) \simeq \mathcal{O}_K$*) and $\mathfrak{P} \mid p$ a prime of FK lying over a place of good reduction. Then E has ordinary reduction mod $\mathfrak{P} \cap F$ if and only if p is split in K. Moreover, if p is split, then the reduction map gives a natural isomorphism* $\mathrm{End}(E) \simeq \mathrm{End}(\overline{E})$.

Proof. Suppose that p is split in K, so $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, Without loss of generality, suppose that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, and let m be the order of $[\mathfrak{p}] \in \mathrm{Cl}(K)$. Then $\mathfrak{p}^m = \mu\mathcal{O}_K$ and $\mathfrak{p}'^{\,m} = \mu'\mathcal{O}_K$ for some $\mu, \mu' \in \mathcal{O}_K$. Up to multiplying by a unit, it follows that $\mu\mu' = p^m$. Moreover, since p is split, we have $\mu' \notin \mathfrak{p}$. We use the notation $[\mu']$ to denote the element of $\mathrm{End}(E)$ corresponding to μ' in the identification $\mathrm{End}(E) \simeq \mathcal{O}_K$. Then $\mu' \notin \mathfrak{p}$, else $\mathfrak{p} = \mathfrak{p}'$, and so we can consider the reduction of $[\mu']$ mod $\mathfrak{p}$. In particular, if ω is a differential on E over F, then we necessarily have

$$[\mu']^*(\omega) = \mu'\omega.$$

In particular, the reduction is nonzero, and so $\overline{[\mu']}$ is separable. Since $\overline{[\mu']}$ has degree a power of p, this shows that E has ordinary reduction.
Conversely, if E has ordinary reduction, then tensoring the p-adic representation

$$\mathrm{End}(E) \otimes \mathbb{Z}_p \to \mathrm{End}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathbb{Z}_p$$

with $\mathbb{Q}$, we get

$$K \otimes \mathbb{Q}_p \to \mathbb{Q}_p.$$

But the left hand side is a 2-dimensional $\mathbb{Q}_p$ algebra, hence the induced map is not injective. But that is only possible if $K \otimes \mathbb{Q}_p$ is not a field, hence p is split in K. □

3. Canonical lifts

There is a generalization of the idea of ordinary reduction to abelian varieties. If A is an abelian variety over a field k of positive characteristic, then

$$A[p](\overline{k}) = (\mathbb{Z}/p\mathbb{Z})^n$$

for some $0 \leq n \leq \dim A$. If $n = \dim A$, so A has as much p-torsion as possible, then we say A is *ordinary*.

If A is an ordinary abelian variety over a perfect field k, then a *canonical lift* of A is an abelian scheme $\mathcal{A}_{/W(k)}$ such that the special fiber of $\mathcal{A}$ is isomorphic to A and the connected-étale sequence of $\mathcal{A}[p^\infty]$ is split. By results of Lubin-Serre-Tate [**?**], the canonical lift of an ordinary abelian variety exists and is unique up to isomorphism.

In the case of an ordinary elliptic curve over $\overline{\mathbb{F}_p}$, Deuring [**?**] gives a classical construction of a canonical lift.

Theorem 3. *Let E_0 be an elliptic curve defined over $\overline{\mathbb{F}_p}$ and $\alpha_0 \in \operatorname{End}(E_0)$ a nontrivial endomorphism, so $\alpha_0 \neq [n]$ for any $n \geq 2$. Then there exists an elliptic curve E over a number field, an endomorphism $\alpha \in \operatorname{End}(\widetilde{E})$, and a prime $\mathfrak{p} \mid p$ such that the reduction of E mod $\mathfrak{p}$ is isomorphic to E_0 and α reduces to α_0.*

Proof. We first notice that we can assume that $\ker \alpha_0$ is cyclic, as otherwise $\alpha_0 = [n] \circ \alpha_0'$ for some other $\alpha_0' \in \operatorname{End}(E_0)$. Similarly, we may assume that $p \nmid \deg \alpha_0$ by considering $\alpha_0 + [n]$ for large enough n prime to p. In both cases, this is simply because lifting $[n]$ is trivial, provided a lift of the curve exists.

Now suppose that α_0 has degree n prime to p. Let $E(j)$ be a generic elliptic curve over $\mathbb{Q}$ with transcendental j invariant. If $Z_1, \ldots, Z_{\psi(n)}$[1] are the cyclic subgroups of $E(j)$ of order n, then we consider the isogenies

$$E(j) \to E(j)/Z_i =: E(j_i).$$

Noting that j_i is integral over $\mathbb{Z}[j]$, we consider the integral closure R of $\mathbb{Z}[j, j_1, \ldots, j_{\psi(n)}]$ in $\mathbb{Q}(j, j_1, \ldots, j_n)$. Then the obvious map

$$\begin{aligned} \mathbb{Z}[j] &\to \overline{\mathbb{F}_p} \\ j &\mapsto j(E_0) \end{aligned}$$

can be extended to R since R is integral and $\overline{\mathbb{F}_p}$ is algebraically closed. Let $\mathfrak{m}$ be the kernel of the extended map $R \to \overline{\mathbb{F}_p}$. We can then choose models for $E(j_i)$ over R with good reduction at $\mathfrak{m}$, so that we can consider the reductions $\overline{E(j_i)}$. In particular, we have that $\overline{E(j)} \simeq E_0$ since they have the same j invariant. Since n is prime to p, the reduction map is injective on n torsion, hence the reductions $\overline{Z_i}$ are again cyclic of order n. By counting, one of the $\overline{Z_i}$, say $\overline{Z_1}$, is equal to the kernel of α_0. Thus

$$\overline{E(j)} \simeq \overline{E(j)}/\overline{Z_1} \simeq \overline{E(j_1)}.$$

[1] Here $\psi(n)$ is the Dedekind psi function $\psi(n) = n \prod_{p|n} \left(1 + \frac{1}{p}\right)$.

So now we have an isogeny between elliptic curves with transcendental j invariant over $\mathbb{Q}$ such that the reductions of the curves are isomorphic and the isogeny reduces to the specified endomorphism. To descend this isogeny to an endomorphism of a curve over a finite extension of $\mathbb{Q}$, we note that the isomorphism $\overline{E(j)} \simeq \overline{E(j_1)}$ forces $(p, j - j_1) \subseteq \mathfrak{m}$.

Pick a minimal prime over $(j - j_1)$, and let $\mathfrak{q}$ be an extension of it to the integral closure $\overline{R}$ in $\overline{\mathbb{Q}(j)}$. We note that $\mathfrak{q} \cap \mathbb{Z} = 0$, else $\mathfrak{q}$ would contain both $j - j_1$ and some rational prime q, hence would have height at least 2.

Quotienting by $\mathfrak{q}$ gives an integral extension of $\mathbb{Z}$, and the reduction $E := E(j)_{\mathfrak{q}}$ and $E(j_1)_{\mathfrak{q}}$ are defined over the fraction field of this integral extension, hence over a number field. Moreover, since $j = j_1$ after quotienting by $\mathfrak{q}$, we have $E(j)_{\mathfrak{q}} \simeq E(j_1)_{\mathfrak{q}}$, potentially after passing to a finite extension so that the isomorphism is defined over the field. Then $\mathfrak{m}/\mathfrak{q}$ gives rise to a place of this field of definition at which the reduction of E is $\overline{E(j)} \simeq E_0$.

Composing the isogeny $\alpha := E \to E(j_1)_{\mathfrak{q}}$ with the isomorphism $E(j_1)_{\mathfrak{q}} \simeq E$, we get an endomorphism $\alpha : E \to E$ with kernel $(Z_1)_{\mathfrak{q}} \simeq Z_1$. Reducing mod $\mathfrak{m}$, we see that the kernel of $\overline{\alpha}$ is $\overline{Z_1}$. Hence $\overline{\alpha}$ and α_0 are isogenies with the same kernel, and so differ by an automorphism. In the general case, the only automorphisms of E_0 are ± 1, which can clearly be lifted, so we are done. If we happen to have E_0 with extra automorphisms, then we necessarily have a curve with j invariant 0 or 1728. But in both cases, we can clearly lift using the standard curves $y^2 = x^3 - x$ and $y^2 = x^3 - 1$ over $\mathbb{Q}$, respectively. □

Returning to the situation of interest, if $E/_{\overline{\mathbb{F}_p}}$ is an ordinary elliptic curve, then Proposition **??** implies that $\mathrm{End}(E) \simeq \mathcal{O}_K$ for some imaginary quadratic field K. Suppose that $\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$ as $\mathbb{Z}$-modules. Then applying Deuring lifting to (E, τ) gives a lift $\widetilde{E}$ over some number field such that $\mathcal{O}_K \subseteq \mathrm{End}(\widetilde{E})$, as the reduction map is injective on endomorphisms. Since the endomorphism ring can't be any bigger than $\mathcal{O}_K$, we conclude that $\mathrm{End}(\widetilde{E}) \simeq \mathrm{End}(E) \simeq \mathcal{O}_K$. So in this case we can actually lift the full endomorphism ring, while this is clearly impossible in the supersingular case.

4. Computation of the local height pairing

The local height pairings $\langle c, T_m d^\sigma \rangle_v$ for each place v of H are computed using intersection theory on Drinfeld's model of $X_0(N)$ over $\mathbb{Z}$. In particular, let $\underline{X} = \underline{X_0(N)}$ be the coarse moduli scheme of $X\mathfrak{X}_0(N)$ and $x = (\phi : E \to E')$ a Heegner point of discriminant D on X over H. If we let Λ_v be the ring of integers in H_v for some place $v \mid p$, then we can work with the corresponding Λ_v-point $\underline{x}$ of $\underline{X} \otimes \Lambda_v$.

Let $\mathcal{A}$ denote the ideal class of K corresponding to $\sigma \in \mathrm{Gal}(H/K)$ via the Artin map, and $r_{\mathcal{A}}(m)$ be the number of integral ideals of norm m. Then the local height pairing can be computed via an arithmetic intersection product.

Theorem 4 ([**?**, Prop. III.3.3])**.** *Assume $m \geq 1$ is prime to N and $r_{\mathcal{A}}(m) = 0$. Then we have the formula*

$$\langle c, T_m d^\sigma \rangle_v = -(\underline{x} \cdot T_m \underline{x}^\sigma) \log q.$$

Working with complete local rings with an algebraically closed residue field will turn out to be useful, so in computing $(\underline{x} \cdot T_m \underline{x}^\sigma)$, we may extend scalars to the completion W of the maximal unramified extension of Λ_v by considering the intersection product on $\underline{X} \otimes_{\Lambda_v} W$.

If S is a complete local ring with algebraically closed residue field k (for example W or W/π^n), and $\underline{x} = (\phi : E \to E')$ and $\underline{y} : (\psi : F \to F')$ are two S-points with noncuspidal reduction, then we define $\mathrm{Hom}_S(\underline{y}, \underline{x})$ to be the set of all pairs of isogenies (f, f') such that the diagram

$$\begin{tikzcd} F \arrow[r, "\psi"] \arrow[d, "f"] & F' \arrow[d, "f'"] \\ E \arrow[r, "\phi"] & E' \end{tikzcd}$$

commutes. The degree of $(f, f') \in \mathrm{Hom}_S(\underline{y}, \underline{x})$ is defined to be $\deg f = \deg f'$. We will often consider the finite set $\mathrm{Hom}_S(\underline{y}, \underline{x})_{\deg m}$ of fixed degree maps.

The main motivation of this lecture is to introduce and start the proof of the following theorem.

Theorem 5 ([**?**, Prop. III.4.4]). *Assume that m is prime to N and $r_{\mathcal{A}}(m) = 0$. Then*

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \frac{1}{2} \sum_{n=1}^{\infty} \# \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma, \underline{x})_{\deg m}.$$

We will only consider the case where p is a split prime in K for now. General reduction theory implies that there is an injection

$$\mathrm{Hom}_{W/\pi^{n+1}}(\underline{x}^\sigma, \underline{x}) \hookrightarrow \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma, \underline{x})$$

and since W is complete, a lifting result implies that

$$\mathrm{Hom}_W(\underline{x}^\sigma, \underline{x}) = \bigcap \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma, \underline{x}).$$

To prove Theorem **??** in the case of a split prime p in K, we will actually show that both sides are identically zero. Since p is split in K, both $\underline{x}$ and $\underline{x}^\sigma$ have ordinary reduction by Proposition **??**. To see that the right hand side is zero, it suffices to show that $\mathrm{Hom}_W(\underline{x}^\sigma, \underline{x}) \simeq \mathrm{Hom}_{W/\pi}(\underline{x}^\sigma, \underline{x})$. Since $\mathrm{Hom}_W(\underline{x}^\sigma, \underline{x})$ can be identified with the set of integral ideals in $\mathcal{A}$, with degree equal to the norm of the ideal, the assumption $r_{\mathcal{A}}(m) = 0$ allows us to conclude $\mathrm{Hom}_W(\underline{x}^\sigma, \underline{x}) = 0$. Since $\mathrm{Hom}_{W/\pi^{n+1}}(\underline{x}^\sigma, \underline{x}) \hookrightarrow \mathrm{Hom}_{W/\pi^n}(\underline{x}^\sigma, \underline{x})$, we can then conclude that every term in the right hand side is zero. Unfortunately the Deuring lifting is only enough to conclude that endomorphism rings over W and W/π are isomorphic, and we need Serre-Tate theory to obtain the isomorphism between the two Hom sets. The computation of the left hand side is shown to be zero by actually computing the intersection product (which will again appeal to the theory of canonical lifts).

References

[Deur] M. Deuring, “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”. *Abh. Math. Sem. Univ. Hamb.* **14** (1941), 197–272.

[GZ] B. Gross, D. Zagier, “Heegner points and deriatives of L-series”, *Inventiones Math.* **84** (1986), 225-320.

[Lang] S. Lang, *Elliptic Functions*, **112**, Springer, (1987).

[LST] J. Lubin, J-P. Serre, and J. Tate, *Elliptic curves and formal groups*, Woods Hole Summer Institute, 1964. (Mimeographed notes.) Available at www.ma.utexas.edu/users/voloch/lst.html.

[Sil1] J.H. Silverman, *The Arithmetic of Elliptic Curves*, **106**, Springer, (1992).