MATH 8120: FINAL PRESENTATION TOPICS

TYLER GENAO

Please email me your top 3 choices of presentation topics by Friday, March 28, 2025.

1. Description

In lieu of having final exams, we will be having final presentations. These will be ~ 30 minute presentations given at the end of the semester. Through this project, you will have the opportunity to explore and present on a topic not fully covered in lecture. These presentations are separate from the homework presentations.

You will have approximately a month to work on your final presentation. If you would like, you can work and present in pairs for your presentation; note that pairs still present for ~ 30 minutes in total. We will have project presentations on the final exam day (Tuesday, April 29 from $4 - 5:45$ PM), as well as on 1 or 2 additional days (we have 11 students enrolled in this class).

Below is a list of possible topics you can present on. Each topic has a short summary meant to give you an overview of the topic, to serve as a loose guideline for your presentation. Most topics have overlap with others. If you would like, you can instead present on a relevant paper on elliptic curves – but keep in mind the proceeding paragraph. If there is a topic in elliptic curves that you are interested in but do not see on the list below, you can also reach out to me about it (Appendix C in [Sil09] gives several more possible topics, e.g. Néron models and Tate's algorithm, L-series, the Sato-Tate conjecture, etc.).

As already noted, one purpose of the final presentations is to present an unexplored, relevant elliptic curves topic to the class. In particular, the talk should not be too technical, and should not assume background we did not cover in class. There are some exceptions to this, such as a talk on abelian varieties – in these cases, you should do your best to make it accessible. Please see the course syllabus for an overview of the topics we will cover in lecture before final presentations (which you can assume as background).

2. Possible Presentation Topics

Project Title	Summary
Abelian varieties	Elliptic curves are unique among algebraic curves, in that the set of their algebraic points is a group. When an elliptic curve E is given in Weierstrass form, this group law is the chord and tangent method. However, we also have an isomorphism $\kappa\colon E \xrightarrow{\sim} \mathrm{Pic}^0(E)$ via $P \mapsto [(P)-(O)]$, where $\mathrm{Pic}^0(E)$ was the *Jacobian,* or degree 0 Picard group, of E. On this Jacobian, the group law is given by addition of divisor classes. As it turns out, there is a larger class of varieties which admit a group structure on their geometric points; these are called *abelian varieties.* One-dimensional abelian varieties are precisely elliptic curves. Abelian varieties also arise as Jacobians of algebraic curves. This talk will focus on some basic constructions of abelian varieties, along with statements of results comparable to those for elliptic curves (possibly noting results which hold for elliptic curves but not more general abelian varieties). You could also talk about explicit examples of abelian varieties as Jacobians of e.g. hyperelliptic curves. This project requires some more familiarity with basic algebraic geometry.
Algorithmic aspects over $\mathbb{F}_q$	This follows Chapter 11 of [Sil09]. As we have seen, there are several interesting computational aspects for elliptic curves over number fields, the primary one being a computation of the Mordell-Weil group $E(F)$. There are also many interesting computational problems for elliptic curves over finite fields, which are connected to cryptography. In this project, you will present results on computations for elliptic curves $E_{/\mathbb{F}_q}$ over finite fields. For example, you can present on fast algorithms for adding points on E, or on determining the size of $E(\mathbb{F}_q)$. You could also present on Lenstra's elliptic curve factorization algorithm, which uses elliptic curves to factorize integers. Or, you could review the elliptic curve discrete logarithm problem (ECDLP) and cryptographic constructions based on its difficulty, as well as situations where certain elliptic curves provide easy answers to ECDLP. This project would pair well with a live code demonstration.

Project Title	Summary
Complex elliptic curves	This follows Chapter 6 of [Sil09]. Over $\mathbb{C}$, an elliptic curve can be realized as a (one-holed) torus, i.e., as $\mathbb{C}$ modulo a rank two $\mathbb{Z}$-lattice: this is the so-called *uniformization theorem* for elliptic curves. Viewing complex elliptic curves as tori allows for a simple description of isogenies and torsion on elliptic curves, among other things. In this project, you will explore the construction of elliptic curves over $\mathbb{C}$ via elliptic functions, and deduce properties of complex elliptic curves and their isogenies, culminating in a description of the uniformization theorem. You can also go over proofs of theorems for complex elliptic curves which are easier over $\mathbb{C}$ than over $\overline{\mathbb{Q}}$ (such as a description of $E[n]$ as a rank two $\mathbb{Z}/n\mathbb{Z}$-module, see [Sil09, Exercise 3.8]).
Complex multiplication	Recall that an elliptic curve $E_{/k}$ has *complex multiplication over k* (or *CM over k*) if $\mathrm{End}_k(E) \supsetneq \mathbb{Z}$. In this case, we know that $\mathrm{End}_k(E)$ is an order $\mathcal{O}$ in either an imaginary quadratic field, or a quaternion algebra over $\mathbb{Q}$. When $\mathrm{char}(k) = 0$, the latter case cannot happen. This project will focus on the case where $F := k$ is a number field. Thus, for a CM elliptic curve $E_{/F}$, we know that $\mathrm{End}(E)$ is an order in an imaginary quadratic field K. Such a "K-CM" elliptic curve provides an *explicit class field theory for K*. Recall the *Kronecker-Weber theorem,* which states that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$. In analogy to this, the torsion points on a K-CM elliptic curve characterize the finite abelian extensions of K. This project will explore the foundational properties of CM elliptic curves; it can explore the description of the class field theory obtained by division fields of CM elliptic curves, as well as Galois representations of CM elliptic curves. See [Sil09, §C.11] and [Sil94, Chapter 2]. See also my older notes on class field theory here.

Project Title	Summary
Division polynomials	It is of great interest to understand torsion points on elliptic curves. One way to understand their rationality is via Galois representations. However, given an elliptic curve E in Weierstrass form, can we determine its torsion points explicitly? One way to do this is by determining the roots of the *division polynomials* of E. These are recursively defined polynomials over $\mathbb{Z}$ with coefficients in terms of the Weierstrass equation for E. In this project, you will define and construct division polynomials for E and prove some basic results for them; see [Sil09, Exercise 3.7], for example. Since division polynomial coefficients can get complicated pretty quick, you could also write and demonstrate a computer program which calculates the n-division polynomial of an elliptic curve. You could also give examples of n-torsion points on specific elliptic curves using n-division polynomials, and compare their fields of definition to what's described by the curves mod-n Galois representation.
Formal groups	This follows Chapter 4 of [Sil09]. The torsion group of an elliptic curve E over a number field F can be analyzed by studying it through a particular short exact sequence of abelian groups, $0 \to E_1(F_{\mathfrak{P}}) \to E_0(F_{\mathfrak{P}}) \xrightarrow{\text{red}} \tilde{E}_{\text{ns}}(k) \to 0$, where $F_{\mathfrak{P}}$ is the completion of F at a nonzero prime ideal $\mathfrak{P} \subseteq F$. A crucial ingredient in analyzing such a SES is that the group $E_1(F_{\mathfrak{P}})$ is a *formal group over R,* where R is the discrete valuation ring of $F_{\mathfrak{P}}$ associated to $\mathfrak{P}$. Thus, understanding formal groups is important when studying elliptic curves over local fields (and consequently number fields). This presentation will focus on presenting some basic results on the arithmetic of *formal groups:* formal groups are "group laws without group elements." As an example, your presentation can culminate in proving results from §4.3 and 4.6 that we have used in class, which describe torsion from the groups associated to formal groups.

Project Title	Summary
Galois representations	Recall that for an elliptic curve $E_{/k}$ and an integer $n \in \mathbb{Z}^+$, the *mod-n Galois representation of E,* written as $\rho_{E,n} \colon G_k \to \mathrm{Aut}(E[n])$, describes the action of G_k on $E[n]$. Similarly, for each prime $p \in \mathbb{Z}^+$ we have the *p-adic Galois representation* $\rho_{E,p^\infty} \colon G_k \to \mathrm{Aut}(T_p(E))$, which describes the action on all p-primary torsion of E. Finally, we have the *adelic Galois representation* $\rho_E \colon G_k \to \mathrm{Aut}(T(E))$, where $T(E) := \varprojlim_{n \geq 1} E[n]$ is a $\hat{\mathbb{Z}}$-module (profinite integers), which packages all of this information together. These representations encode important information about the rationality of torsion points on E. We have seen already that if E has CM and $p \neq \mathrm{char}(k)$, then $\rho_{E,p^\infty} \colon G_k \to \mathrm{GL}_2(\mathbb{Z}_p)$ is abelian; thus, it never surjects. However, in the case where $F := k$ is a number field and $E_{/F}$ is non-CM, a theorem of Serre shows that $\rho_{E,p}(G_F) = \mathrm{GL}_2(\mathbb{F}_p)$ for all but finitely many primes $p \in \mathbb{Z}^+$; this is equivalent to $\rho_{E,p^\infty}(G_F) = \mathrm{GL}_2(\mathbb{Z}_p)$ for all but finitely many p, which is iff $\rho_E(G_F)$ is open in $\mathrm{GL}_2(\mathbb{Z})$. This project explores aspects of Serre's open image theorem, and the image of elliptic curve Galois representations. For example, one can explore the proof of Serre's theorem; or the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ and their implication on torsion of elliptic curves; or the discrepancies between CM and non-CM Galois representations (there are a lot of good papers on this!). Here is a translation of Serre's 1972 paper from French. Here are my old notes on his paper.
Integral points	This follows Chapter 9 of [Sil09]. When studying rational points on curves, it is interesting to ask what is known about integral points. Siegel has shown that a curve given by a rational Weierstrass equation has finitely many integral points. This presentation will focus on either of the two proofs given by Siegel (see §9.3 and §9.4); the latter proof reduces to studying S-unit equations. This talk can discuss effective versions of Siegel's theorem (see §9.5), or determining integral points on specific families of curves, such as those in §9.6.

Project Title	Summary
Modular curves	*Modular curves* are a certain class of algebraic curves defined over number fields, whose points, loosely speaking, are elliptic curves with a fixed torsion structure. For example, for an integer $n \in \mathbb{Z}^+$, the modular curve $X_1(n)_{/\mathbb{Q}}$ is a moduli space whose closed points have the form $x = [E, P]$, where $P \in E$ has order n; while the modular curve $X_0(n)_{/\mathbb{Q}}$ is a moduli space whose closed points have the form $x = [E, C]$, where $C \subseteq E$ is a cyclic subgroup of order n. A point $x = [E, P]$ on $X_1(n)$ (resp. $y = [E, C] \in X_0(n)$) is e.g. $\mathbb{Q}$-rational iff E has a model over $\mathbb{Q}$ and P is $\mathbb{Q}$-rational (resp. iff E has a model over $\mathbb{Q}$ and C is $G_{\mathbb{Q}}$-stable). Ultimately, each modular curve X has an associated level n and subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for which F-rational points on X correspond to elliptic curves over F whose mod-n Galois representation over F is contained in H, up to conjugacy. Modular curves have been extremely useful in proving results about rational torsion *uniformly*. For example, Mazur has shown that $X_1(p)$ has no noncuspidal $\mathbb{Q}$-rational points if p is a prime > 7; with this, he was able to give a complete classification of torsion groups over $\mathbb{Q}$. Ultimately, modular curves allow us to utilize powerful algebro-geometric techniques to prove uniformity results for the arithmetic of elliptic curves. This project explores the construction of modular curves via congruence subgroups, and/or their application towards proving uniformity results on elliptic curve Galois representations. See [Sil09, §C.13] and [DS05]. For another introduction to modular groups, see here.
Ordinary vs. supersingular	This follows §5.3 and 5.4 of [Sil09]. We have shown that for any elliptic curve E, its endomorphism ring is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra over $\mathbb{Q}$. When $\mathrm{char}(k) = 0$, only the first two cases can happen. However, when k is a finite field, we always have $\mathrm{End}(E) \supsetneq \mathbb{Z}$. This presentation will focus on understanding $\mathrm{End}(E)$ more closely when k is a finite field. You will prove the main theorem of §5.3, which gives equivalent conditions for characterizing $\mathrm{End}(E)$ as either an order in an imaginary quadratic field, or as an order in a quaternion algebra over $\mathbb{Q}$ (*ordinary* vs. *supersingular*) (you don't have to describe the formal group height). Then in §5.4, you can describe and prove results which concern ordinary and supersingular primes for elliptic curves, maybe even describing the more theoretical conjectures.

Project Title	Summary
Selmer and Shafarevich-Tate groups	This talk will focus on Chapter 10 of [Sil09] (realistically, we will only cover up to §10.1 before the semester ends). As we will see in class, given an elliptic curve E over a number field F, computing the Mordell-Weil group $E(F)$ amounts to computing $E(F)$[tors] – which we can do through computations over local and finite fields – and then computing $E(F)/mE(F)$. This can be done via making the proof of the weak Mordell-Weil theorem explicit. For example, taking $m := 2$, this is done via 2-descent; we reduce to checking locally for rational points on twists of E called *homogeneous spaces.* An obstruction to the procedure above is the fact that a homogeneous space can have a rational point over every completion of F, and yet no F-rational point. This would be a failure of the *local-global principle;* the success/failure of the local-global principle for homogeneous spaces is measured by the *Shafarevich-Tate group* of E. This talk will focus on describing this group, as well as the *Selmer group;* both arise when trying to compute $E(F)/mE(F)$. You can then survey recent papers on computing these two groups; alternatively, you can focus on computing these groups for certain families of elliptic curves (such as those in §10.6 from [Sil09]).

References

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York (2005).

[Sil94] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York (1994).

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, 2nd Ed., Graduate Texts in Mathematics, vol. 106, Springer (2009).