Math 719: Asymptotic Problems in Number Theory
Summary of Lectures- Spring 2015.

In this document I will give a summary of what we have covered so far in the course, provide references, and given some idea of where we are headed next.

1 Lecture 1

In the first lecture I gave an overview of what we will cover in the first half of the course. The broad goal is to understand the behavior of families of arithmetic objects. We want to understand what an 'average' object looks like, and also what an 'extremal' object looks like. We will look at this question in a few different settings. The three main topics will (likely) be:

1. Class groups of imaginary quadratic fields;
2. Curves over finite fields;
3. Linear codes.

Our first major goal is to understand positive definite quadratic forms of given discriminant and then connection to class groups of the field $\mathbb{Q}(\sqrt{-d})$, or really more accurately, the quadratic ring of discriminant $-d$. We will spend approximately the first three weeks setting up this connection, first focusing on quadratic forms and then transferring over to ideal class groups.

As we vary over all quadratic imaginary fields $K = \mathbb{Q}(\sqrt{-d})$ where $d > 0$ is squarefree, we get some set of finite abelian groups $C(\mathcal{O}_K)$. What can we say about these groups? How large are they on average? How often is this group trivial? What can we say about the p-parts of these groups for fixed p?

Understanding these questions will require using some of the key ideas of class field theory and also understanding some analytic techniques. To answer the question about average size we will introduce the Dedekind zeta function of a number field and discuss Dedekind's class number formula. The Stark-Heegner theorem gives a complete answer to the second question, a complete list of d such that $\mathbb{Q}(\sqrt{-d})$ is a unique factorization domain. For the third question we will investigate the Cohen-Lenstra heuristics, which roughly state that a group should arise in proposition to the inverse of its number of automorphisms.

The prime $p = 2$ behaves differently from odd primes with respect to p-parts of class groups. We will discuss genus theory, both on the quadratic forms side and on the ideal class group side in order to understand this special behavior. The only other proven case of the Cohen-Lenstra heuristics is the average number of 3-torsion elements in $C(\mathcal{O}_K)$. This comes from counting cubic fields of

bounded discriminant and a little bit of class field theory. We will prove this result, the Davenport-Heilbronn theorem, and discuss related questions about counting number fields and the orders they contain.

2 Lecture 2

In the first half of this lecture we discussed the other two main topics that we plan to cover in this course. How many points can a smooth genus g curve over a finite field $\mathbb{F}_q$ have? We call this number $N_q(g)$. We can try to compute this number for particular values of (q, g), or we can try to understand its asymptotic behavior. We consider the quantity

$$A(q) = \lim_{g \to \infty} \sup \frac{N_q(g)}{g}.$$

We will discuss elliptic curves over finite fields, the case $g = 1$, where we know $N_q(1)$ for all q. We can also try to understand the 'average' behavior of all elliptic curves over a fixed field $\mathbb{F}_q$. As $q \to \infty$ work of Birch, building on fundamental results of Deuring in the theory of complex multiplication gives a nice answer. This is the 'vertical' Sato-Tate theorem for elliptic curves. We will give a detailed sketch of the proof.

Hasse's theorem tells us that an elliptic curves over $\mathbb{F}_q$ has $q+1-t$ rational points, where $|t| \leq 2\sqrt{q}$. We can see that this cannot be improved. The Hasse-Weil bound is the analogue for higher genus curves, and here there are interesting and subtle questions about upper bounds for $N_q(g)$. We will discuss zeta functions of curves, the Weil conjectures for curves, and improvements to the Hasse-Weil bound. We will also discuss the cases of $g = 2$ and $g = 3$.

In a different direction, we will discuss curves like the Hermitian curve over $\mathbb{F}_{q^2}$ which has very many rational points and a very large automorphism group given its genus. We will also discuss the theorem of Ihara / Tsfasman-Vladut-Zink which gives an asymptotic lower bound for $A(q)$ by studying rational points on modular curves over finite fields.

We also introduced some basic problems in coding theory. How large can a code over $\mathbb{F}_q$ of length n be if the minimum distance of the code is at least d? What if we restrict to linear codes? We will discuss both upper bounds and lower bounds. These lower bounds will often come from algebraic constructions, evaluating vector spaces of polynomials at specified points. In particular, we will discuss algebraic geometry codes, and more specifically the Goppa codes that generalize the classical Reed-Solomon and Reed-Muller codes. These codes come from taking an algebraic curve and a divisor D, and evaluating every polynomial in the Riemann-Roch space $L(D)$ at a specified set of points.

For the rest of this lecture we shifted to talk about the basics of integral binary quadratic forms. For this part of the course (approximately the first three or four weeks) I will closely follow parts of Cox's book *Primes of the form* $x^2 + ny^2$. It is not available as an online resource for Yale students, but I hope that you are able to get a copy.

In this lecture we first introduce some of the basic terminology of binary quadratic forms. I closely followed 2.A of Cox for this. We basically did everything up to Theorem 2.8, but also phrased quadratic forms in terms of matrices.

3 Lecture 3

In lecture 3 we started by introducing reduced quadratic forms. I sketched the proof of Theorem 2.8 of Cox, that every primitive positive definite form of discriminant $D < 0$ is properly equivalent to a reduced one. An easy consequence of the definitions is that there are only finitely many reduced forms of given discriminant. This number is called the class number, or 'form class number' $h(D)$. We call the set of all classes $C(D)$. Later we will show that this is a group.

We then defined the genus of a quadratic form of discriminant D in terms on the set of values represented by $(\mathbb{Z}/D\mathbb{Z})^*$. We introduced the homomorphism χ, which is defined in Lemma 1.14 of Cox. The results about genera we talked about are in Cox 2.C. In particular, we proved Theorem 2.16. We then sketched Landau's argument for the set of all $D \equiv 0 \pmod 4$, $D < 0$ such that $h(D) = 1$. This is Theorem 2.18. We gave two examples of genera and showed how when each genus consists of a single class we get nice corollaries about representation of integers by quadratic forms. The examples we gave are on page 30 of Cox. We defined the principal form and sketched the proof of Lemma 2.24, showing that the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal genus form a subgroup, and that every other genus gives a coset. We stated the fact that the map taking a class to the coset represented by its genus is a group homomorphism, but in order to make that rigorous we need $C(D)$ to be a group. Once you believe that $C(D)$ is a group, Lemma 3.13 shows that Dirichlet composition makes this map into a group homomorphism.

4 Lecture 4

We started with a review of everything about forms of discriminant D up to this point. We then defined Gauss composition and stated that it makes $C(D)$ into a group. We defined Dirichlet composition, which is much more explicit and easier to compute with. This is all done in the first section of 3.A in Cox. There are a lot of details to check, but it is worth going through and checking some of this at least once.

In the last part of the lecture we discussed Bhargava's work on Gauss composition using $2 \times 2 \times 2$ cubes. I first talked about how to slice a cube in three different ways, which gives three pairs of 2×2 matrices. For each pair we get a quadratic form. It is a fact that I did not prove that each of these forms has the same discriminant. You can just check this by writing down the forms explicitly in terms of the eight entries of the cube and actually taking the determinants.

I described another way of thinking about this in terms of an explicit basis of $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^2$ so that a cube gives an element of this space. We have an action of $G = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$

on this space, and so we also have an action on cubes. We need only understand the action by $\gamma \times I \times I$ (and the permutations of this) where we extend things in the obvious way. So an element of G acts on a cube, and an element of G also acts on our triple of quadratic forms. We stated a major theorem, that this action 'commutes'. We also stated the correspondence between G-orbits on this vector space of cubes and the set of isomorphism classes of pairs (S, I_1, I_2, I_3) where S is a quadratic ring and (I_1, I_2, I_3) are a balanced triple of 'oriented ideals' of S.

There are a few good references for this material. I highly recommend Dick Gross' Fields Medal Laudation for Bhargava. It is available on Youtube:
`https://www.youtube.com/watch?v=1wfv_RImVdI`

Here is a link to Bhargava's original paper on Gauss composition:
`http://annals.math.princeton.edu/wp-content/uploads/annals-v159-n1-p03.pdf`

Here is a link to Bhargava's ICM notes on this topic:
`http://icm2006.mathunion.org/proceedings/Vol_II/contents/ICM_Vol_2_13.pdf`

I have also put Bhargava's original paper and his 2006 ICM notes onto Classesv2 under the resources tab. Finally, here is a link to an article giving a summary of these topics that contains some explicit computations:
`http://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer/gauss_composition.pdf`

5 Lecture 5

In this lecture I started with some basic algebraic number theory. My favorite reference for Algebraic Number Theory is the book (with that title) by Fröhlich and Taylor. I am mostly pulling statements from this text, so you can look there for complete proofs. I introduced the ring of algebraic integers, number fields, what it means for a field to be perfect, and stated that all finite fields and fields of characteristic zero are perfect.

I talked about the degree of a field extension. If we have L/K then the degree of the extension is the degree of L over K as a vector space. I stated this in a confusing way in lecture. I also stated that the number of distinct embeddings of a degree d number field K into $\mathbb{C}$ is exactly d. If I had it to do over again I would have explained this as it is explained in the Algebraic Number Theory course notes of Tom Weston:
`http://people.math.umass.edu/~weston/cn/notes.pdf`
He begins with the example of quadratic fields but states the necessary facts about complex embeddings in the first few pages. I stated the primitive element theorem and explained that the degree of the minimal polynomial also corresponds to the degree of a field extension. I stated what it means for a ring to be integrally closed in its field of fractions and that the ring of integers of a number field is a Dedekind domain.

We defined fractional ideals and $\mathfrak{o}$-ideals. I made a mistake in this discussion that Jeremy pointed

out. I meant to say that if $\mathfrak{b}$ is a *finitely generated* $\mathfrak{o}$-submodule of K, then it is of the form $c \cdot \mathfrak{a}$ with $\mathfrak{a}$ an $\mathfrak{o}$-ideal. I left out the words finitely generated which led to some confusion. My bad.

We then defined the product of fractional ideals, principal fractional ideals, and stated three theorems: every nonzero ideal $\mathfrak{a}$ of a Dedekind domain $\mathfrak{o}$ can be written uniquely up to order as a product of prime ideal of $\mathfrak{o}$, every fractional ideal of a Dedekind domain is invertible, and every ideal of a Dedekind domain can be generated by two or fewer elements. Shaked asked a nice question about this last statement, which is, when do you ever use such a thing, and Sabrina suggested that it's useful when you actually want to do computations. We will see soon that there are at most finitely many ideals of norm at most X in a given ring of integers $\mathcal{O}_K$, and knowing something about the possible generating sets let's us write them all down. I did a little searching about this and found a nice MathOverflow question related to this topic:
`http://mathoverflow.net/questions/12969/non-dedekind-domain-in-which-every-ideal-is-generated-`
(I know this runs off the line, but if you click the link it takes you to the question.)

We went on to define the ideal class group $\mathrm{CL}(\mathcal{O}_K)$ of fractional ideals modulo principal fractional ideals and noted that $\mathcal{O}_K$ is a principal ideal domain if and only if the class group is trivial. We stated two simple propositions, that every ideal class contains a $\mathfrak{o}$-ideal and that two $\mathfrak{o}$-ideals $\mathfrak{a}_1, \mathfrak{a}_2$ are in the same class if and only if there exist elements a_1, a_2 such that $\mathfrak{a}_1 a_1 = \mathfrak{a}_2 a_2$.

We stated the theorem that every ideal class contains infinitely many prime ideals. Owen made a comment this, asking how this is related to results about distributions of primes. I also found a nice MathOverflow question related to this:
`http://mathoverflow.net/questions/29190/dirichlets-theorem-for-number-fields`

Finally, we put the class group into a nice exact sequence by identifying it with the cokernel of the map that takes $\alpha \in K^*$ to the principal fractional ideal that it generates. We stated Dirichlet's Unit Theorem about the structure of $\mathcal{O}_K^*$. I was a little unclear about exactly what a *fundamental unit* should be. When the group of units is rank 1 a fundamental unit is any generator of the unit group (modulo roots of unity). I stated Gauss' class number one problem for real quadratic fields, that it is conjectured that there are infinitely many squarefree $d > 0$ such that $\mathbb{Q}(\sqrt{d})$ has class number one, and that in fact, the Cohen-Lenstra heuristics imply that approximately 75% of real quadratic fields should have this property. I started to discuss finiteness of the ideal class group, which I will cover more carefully in the next lecture.

For this lecture I would recommend Sections 1.1, 1.2, and 2.1 of Fröhlich and Taylor. Dirichlet's Unit Theorem is proven in Section 4.4. I will also point out that a lot of this material is covered more quickly in Chapter 5 Section A of Cox, but with no proofs (though there are specific references for proofs). Similarly, Ireland and Rosen *A Classical Introduction to Modern Number Theory* gives a fast introduction to this subject with few proofs.

6 Lecture 7

I started this lecture by going over some of the basics of ideal decompositions in field extensions. This led to another proof that there are only finitely many ideals of bounded norm in $\mathcal{O}_K$. I then went on to discuss the finiteness of the class group using Blichfeldt's lemma. This closely follows the approach in Chapter 7 of Stein's Algebraic Number Theory:
`http://wstein.org/books/ant/ant.pdf`

I apologize for the confusion during lecture about the proof. If you would like a more explicit discussion of what subset to choose as S, you can look at the similar approach to this material given in de Shalit's Algebraic Number Theory notes, Theorem 1.1 of Chapter 2, specifically equation (1.7) on page 21:
`http://www.ma.huji.ac.il/~deshalit/new_site/files/NTcourse.pdf`

7 Lecture 8

We sketched the geometry of numbers proof of Hermite's theorem that the number of number fields K of with absolute value of the discriminant at most X is finite. This proof is given on page 12-13 of the del Shalit reference above. Since we have now seen that the absolute value of the discriminant of K is larger than 1 for every $K \neq \mathbb{Q}$, we will know that in every K at least one rational prime ramifies as soon as we know that a rational prime p ramifies in K if and only if p divides the discriminant. This is Theorem 1.3 on p. 31 of the de Shalit reference (and is contained in several other sources as well.)

We discussed the 'relative discriminant' of a field extension and stated (but did not prove) the analogous result about prime ramification. This theorem is in Fröhlich and Taylor, among other places..

We discussed the logarithmic embedding of $\mathcal{O}_K^\times$ into $\mathbb{R}^{r+s}$ and use it to define the regulator of K, which plays an important role in asymptotic growth questions about fields. We sketched how this embedding and geometry of numbers ideas are used to prove Dirichlet's Unit Theorem.

We then transitioned back to talking about quadratic fields, stating some of the most basic results. We defined the concept of an order $\mathcal{O} \subset \mathcal{O}_K$ and proved some basic facts about them following the beginning of Chapter 7 in Cox. Since orders are not generally Dedekind domains we no longer have unique factorization of ideals and it is no longer true that every fractional ideal is invertible. We introduced proper ideals to try to salvage these properties and showed that a fractional ideal is invertible if and only if its proper. This is Proposition 7.4 in Cox.

8 Lecture 9

We started by defining the ideal class group of an order. We stated the main theorem relating the ideal class group of an order to the corresponding form class group and gave a sketch of the proof. This is Theorem 7.7 in Cox.We briefly discussed how these ideas can be adapt to real quadratic fields and indefinite quadratic forms where the relationship is not quite so clear. We then started to discuss ideals prime to the conductor. This is because class field theory is usually phrased in terms of the maximal order of a field, so we would like to find a way to understand the class group of an order that deals only with ideals in the maximal order.

9 Lecture 10

We discussed genus theory for positive definite quadratic forms following Chapter 3 Section B of Cox. We sketched the proofs of the main results, counting the number of genera of forms of a given discriminant and describing the principal genus as the subgroup of ideal classes that are squares. We introduced the concept of an assigned character and briefly discussed different notions of the equivalence of forms. A great reference for this topic is Conway's short book *The Sensual Quadratic Form*.

We introduced some basic ideas necessary for class field theory and then stated the main theorem that we will use next time- decomposition group, inertia group, unramified extension, etc. This is all in Chapter 5 of Cox.

10 Lecture 11

We defined the Hilbert class field L of a number field K, the Artin symbol, and the Artin map. We stated the main theorem that we will use, that the Artin map gives an isomorphism between $\mathrm{Gal}(L/K)$ and the ideal class group of K. We stated the analogous result for orders. These results come from Chapter 6 of Cox which does not give proofs. Cassels and Fröhlich *Class Field Theory* is a great reference.

We looked at the case of S_3 extensions of $\mathbb{Q}$ and described the connection between unramified cubic extensions of an imaginary quadratic field and three torsion elements in the class group. We briefly discussed results on the 3-rank of quadratic fields. We stated the Davenport-Heilbronn theorem. Melanie Matchett Wood's Arizona Winter School notes from 2014 are a great reference for the discussion of cubic fields and the Davenport-Heilbronn theorem. We also briefly discussed genus theory for fields in terms of unramified extensions and the genus field.

11 Lecture 12

We followed Matchett Wood's notes pretty closely during this lecture. We discussed statistics of class groups, and in particular the Cohen-Lenstra heuristics for the Sylow p-subgroups of ideal class groups of imaginary quadratic fields. We talked about this measure on finite abelian p-groups and its moments, and the moments in terms of the expected number of surjections to a fixed abelian group. We gave several instances where Cohen-Lenstra type behavior is expected to hold.

12 Lecture 13

We discussed some analytic results related to class numbers of imaginary quadratic fields. We first stated the asymptotic for the sum of $h(D)$ taken over all D between $-X$ and 0. This is a theorem of Mertens/Lipschitz that was conjectured by Gauss. We described a geometry of numbers proof that works by estimating the number of lattice points in a certain expanding region. We stated the analogue in the real case, which compute the sum of the class number times the regulator. This is a theorem of Siegel. Gross briefly discusses these results in his ICM intro for Bhargava's Fields Medal.

We then introduced the Dedekind zeta function of a number field and stated the Dirichlet class number formula. We talked about how in the abelian case this zeta function factors as a product of Dirichlet L-functions. We discussed some basic properties of these L-functions in an attempt to explain why the special value $L(1, \chi)$ should be related to class numbers. We sketched the argument for Dirichlet's theorem on primes in progressions. We then gave a detailed sketch of the proof of the class number formula for imaginary quadratic fields by computing the total number of representations of an integer n by all primitive positive definite reduced forms of discriminant d in two different ways. First we ended up counting lattice points in an expanding ellipse, which can be well-approximated by the area. Second, we worked with sums of the Jacobi symbol, which led to an expression involving $L(1, \chi)$. This lecture closely followed parts of Davenport's book *Multiplicative Number Theory*, first Chapters 1 and 2, and then Chapter 6 on the class number formula.

13 Lecture 14

Geoff told us about Bhargava's work on Gauss composition via $2 \times 2 \times 2$ cubes and some of its generalizations.

14 Lecture 15

I briefly discussed Siegel's theorem about lower bounds for $L(1,\chi)$ following Chapter 6 of Davenport. The main idea is to prove a certain zero-free region for $L(s,\chi)$ and then control the growth of $L'(s,\chi)$ near $s=1$. I sketched an argument due to Estermann that is given in detail in that reference. This result combined with the Dirichlet class number formula from last time tells us that as $d \to -\infty$ the class number of the order of discriminant d is approximately $|d|^{1/2}$. This tells us that $h(d)$ must get large, and in particular that $h(d) = 1$ for finitely many negative values of d. However, the lower bound we get on $L(1,\chi)$ is ineffective, which means we cannot write down an explicit $D > 0$ for which we know $h(d) > 1$ when $d < -D$. This is related to the Siegel zero, one of the big mysteries of analytic number theory (which would make a very interesting final project presentation). On April 21st, Sabrina will tell us about how to get around this issue to prove the Stark-Heegner theorem, giving the complete list of $d < 0$ such that $h(d) = 1$. We also briefly discussed how the class number of an order can be expressed in terms of the class number of the maximal order containing it. Finally, we stated the analogue for higher degree fields, the Brauer-Siegel theorem on the growth of the class number times the regulator.

We then started discussing the next big topic of the course, curves over finite fields. We started by discussing the Weil conjectures about rational points on varieties over finite fields. I was definitely a little imprecise here because even giving a complete statement involves some more advanced algebraic geometry that we have not covered. I defined the zeta function of a variety over $\mathbb{F}_q$ which is a generating function that tells you the number of points on the variety over all finite extension of $\mathbb{F}_q$. The Weil conjectures tell us that this function satisfies a number of amazing properties, that it is a rational function satisfying a functional equation, and where we know the magnitude of the roots of the polynomials defining this rational function. We explained how this result on the magnitude of the roots gives the analogue of the Riemann-hypothesis. The last part of the Weil conjectures explains how the degrees of these polynomials are related to the Betti numbers of the variety.

We considered some basic examples include affine and projective space and briefly discussed the particular case of algebraic curves. We showed how the Weil conjectures for curves leads to the Hasse-Weil bound for the number of points on a genus g curve over $\mathbb{F}_q$.

There are a number of good references for this section of the course. The first thing I would recommend is Appendix C of Hartshorne. Popa also has very nice notes that go into much more detail than I did which are available here:
`http://homepages.math.uic.edu/~mpopa/571/chapter2.pdf`

Starting in the next lecture we will talk about how the Hasse-Weil bound can be improved. My favorite reference here is the survey article of Voight:
`https://math.dartmouth.edu/~jvoight/articles/pointscurves-moscow.pdf`

15 Lecture 16

How many points can a genus g curve over a finite field $\mathbb{F}_q$ have? Last time we saw how the Weil conjectures for curves lead to the Hasse-Weil bound. We first investigated whether this bound is ever an equality, when $|X(\mathbb{F}_{q^r})| = q^r + 1 + 2q^{r/2}$. Such curves are called maximal. We gave the example of the Hermitian curve and briefly discussed some of its properties. We stated Serre's result that if a curve is 'covered' by an $\mathbb{F}_q$-maximal curve, then it is also $\mathbb{F}_q$-maximal. This leads to many maximal curves that can be constructed from the Hermitian curve by taking the quotient with respect to a subgroup of automorphisms. We also stated a recent result showing that over any $\mathbb{F}_{\ell^6}$ there are maximal curves not isomorphic to a quotient of the Hermitian curve.

We then asked whether the Hasse-Weil bound can be improved in general. We proved Serre's bound, a slight variation where $\lfloor 2g\sqrt{q} \rfloor$ is replaced by $g\lfloor 2\sqrt{q} \rfloor$. We then proved Ihara's bound which is better than Serre's when the genus is large relative to q. This involves relating the expressions for $|X(\mathbb{F}_q)|$ and $|X(\mathbb{F}_{q^2})|$. We stated the Drinfled-Vladut bound which is more complicated but is much better as g does to infinity with q fixed.

We then briefly discussed a geometric approach to bounding $|X(\mathbb{F}_q)|$ due to Stöhr and Voloch. Their results can be used to give another proof of the Hasse-Weil bound and give improvements in many cases. Given a projective nonsingular curve in $\mathbb{P}^n$ defined over $\mathbb{F}_q$ we can define the tangent hyperplane H at each point P. One idea is to study the set of points for which $\varphi(P)$ is in H where φ denote the Frobenius map. This clearly holds for each $\mathbb{F}_q$-rational point, but also can hold for some points defined over finite extensions of $\mathbb{F}_q$. The equation of H is defined by the vanishing of a certain 'Wronskian-type' determinant. The approach involves more geometry than we have covered up to this point- linear series on curves and Weierstrass semigroups.

We briefly explained what Weierstrass semigroups are. Given a point on a curve we consider rational functions regular away from this point. The possible pole orders of these functions form a semigroup $S \subset \mathbb{N}$ and it is a theorem of Weierstrass that $|\mathbb{N} \setminus S| = g$, the genus of the curve. A point such that this semigroup is not $\{0, g+1, g+2, \ldots\}$ is called a Weierstrass point. These Weierstrass semigroups can reveal quite a lot of information about the geometry of the curve. For example, a curve is hyperelliptic if and only if every one of its Weierstrass points has semigroup $\{0, 2, 4, \ldots, 2g, 2g+1, \ldots\}$. My favorite reference for Weierstrass points is Geometry of Algebraic Curves (ACGH). For this approach to bounding rational points on curves I would recommend the original paper or the exposition of Torres.

16 Lecture 17

We briefly discussed the cohomological view of the Weil conjectures. The $\mathbb{F}_q$-rational points of $\mathbb{P}^n$ are those fixed by the Frobenius morphism. So we would like to have a way to understand the number of fixed points of this map. We briefly recalled the Lefschetz fixed-point theorem from algebraic topology which gives a formula related to fixed-points in terms of an alternating sum of

trace of the map induced on the different singular homology groups. We would like to have an analogue here for a variety defined over a finite field, but singular homology is no longer the right setting. We need a new cohomology theory which is called a 'Weil cohomology theory'. This is given to us in the form of ℓ-adic cohomology and one approach to studying the Weil conjectures is to prove that there is a similar formula, the Grothendieck-Lefschetz trace formula, that expresses the number of fixed points of Frobenius in terms of the action of the map induced on the various ℓ-adic cohomology groups. Hartshorne, Popa's notes, and various other advanced references address these ideas. We then showed how to express the generated function attached to powers of traces of a map in terms of the determinant of a certain map. Ultimately this will give us a nice interpretation of the polynomials appearing the rational function expression for the zeta function in terms of the determinant of a map related to Frobenius acting on ℓ-adic cohomology groups.

We then switched gears to talk about one very concrete case, elliptic curves. The Hasse-Weil bound here is actually due to Hasse. This is a case where we can very concretely explain the form of the quadratic polynomial appearing in the numerator of the rational function expression for the zeta function. This will explain why we often right $|E(\mathbb{F}_q)| = q + 1 - t$. The integer t is the 'trace of Frobenius', more precisely, the trace of the map induced by Frobenius on the ℓ-adic Tate module of E where ℓ is a prime distinct from the characteristic of $\mathbb{F}_q$.

We started by recalling some basics of the theory of elliptic curves. We defined isogenies and endomorphisms, torsion points, the dual isogeny, and the Tate-module. We stated some fundamental results about the classification of endomorphism rings of elliptic curves and Tate modules.

There are lots of great references on the basics of the theory of elliptic curves. My favorite is Silverman's book. Much of what we will need is covered in Chapters 3 and 5.

17 Lecture 18

We began by being a little more careful and some of the concepts we introduced last time, defining the degree and separable degree of an isogeny. We explained how our goal is to understand the size of the kernel of $1 - \varphi$, which is equal to its degree. We stated that this can be understood in terms of the trace and determinant of the action of φ on $T_\ell(E)$. We showed how this can be used to express the zeta function of the curve.

We now see that Frobenius is an endomorphism not equal to one of the multiplication by m maps and which satisfies a quadratic polynomial in the endomorphism ring. In this way we see that the endomorphism ring contains an order in a quadratic imaginary field. We then stated several criteria that are equivalent to a curve being supersingular. We defined the j-invariant of a curve and explained what it means for two curves in short Weierstrass form to be isomorphic. We stated Tate's isogeny theorem. We set of the problem of determining $N(t)$, the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves with $E(\mathbb{F}_q) = q + 1 - t$.

18 Lecture 19

Rodrigo gave a lecture about Tate-Shafarevich groups of elliptic curves. These are certain (conjecturally finite) groups related to the group of rational points on the elliptic curve. There is a conjecture that these groups obey a Cohen-Lenstra type distribution, but since these groups carry additional algebraic structure the distribution is a little more complicated.

19 Lecture 20

In this lecture we discussed the 'vertical' version of the Sato-Tate theorem. We started by stating Deuring's result on $N(t)$. The answer is given in terms of a certain sum of class numbers of orders in imaginary quadratic fields, the Kronecker class number of a discriminant. Taking this as our starting point, we normalize a little and can ask interesting asymptotic questions about $N(t)$. That is, let $|E|^* = \frac{|E(\mathbb{F}_q)|-(q+1)}{2\sqrt{q}}$. Hasse's theorem says that $|E|^* \in [-1,1]$. There are approximately $2q$ isomorphism classes of elliptic curves over $\mathbb{F}_q$. As we let q go to infinity, what is the probability that a randomly chosen isomorphism class has $|E|^*$ in the interval (a,b)? The answer is given by the 'vertical Sato-Tate theorem', which is due to Birch. The main idea is to use the Selberg trace formula to relate the sum of class numbers described in the above paragraph to traces of Hecke operators acting on spaces of cusp forms for $\mathrm{SL}_2(\mathbb{Z})$. You can then use basic estimates for the size of these traces to compute the moments of this distribution and show that they match up with the moments of the Sato-Tate distribution.

We also briefly discussed the relationship between this theorem and the Sato-Tate theorem for a fixed elliptic curve over $\mathbb{Q}$. That is, if we take an elliptic curve E and consider the reduction of E to $\mathbb{F}_p$, letting $|\overline{E}(\mathbb{F}_p)| = p+1-a_p$, then how do these a_p vary as we let p go to infinity? The answer is different based on whether E has complex multiplication. The complex multiplication case is far easier, which basically comes from the fact that the L-function attached to such a curve factors as a product of two Hecke L-functions, which are easier to understand. When E does not have complex multiplication this is a much more difficult and recent theorem of Taylor and several collaborators.

20 Lecture 21

Sabrina gave a lecture about the Stark-Heegner theorem which gives the full list of negative integers d such that $h(d) = 1$. Early in the semester we used facts about positive definite quadratic forms to deal with the $d \equiv 0 \pmod 4$ case. The $d \equiv 1 \pmod 4$ case is much more complicated. One first step is to use the relationship between the class number of $\mathcal{O}_K$ and the orders $\mathcal{O}$ it contains to reduced to studying only class numbers of maximal orders. We can also use genus theory to reduce to studying only class numbers of fields with discriminant equal to $-4p$ where p is prime. Sabrina outlined the major necessary results about complex multiplication, introduced the class equation

and Weber functions, and then gave a proof of the theorem. There are several nice references for this material including Cox's book, and the minor thesis of Chao Li, which is available here: `http://www.math.harvard.edu/~chaoli/doc/MinorThesis3.html`

21 Lecture 22

In my final lecture I addressed two topics. I first defined $A(q)$, the limit as g goes to infinity of the maximum number of points on a genus g curve over $\mathbb{F}_q$ divided by g. I gave a sketch of the proof of the Drinfeld-Vladut bound showing that $A(q) \leq \sqrt{q} - 1$. In fact, when q is square this is an equality. This is a theorem of Tsfasman, Vladut, and Zink. One particularly nice set of curves that prove this theorem are the modular curves $X_0(\ell)$ where $\ell \equiv 11 \pmod{12}$ is prime. It is a simple computation using the Riemann-Hurwitz formula that the genus of such a curve is $\frac{\ell+1}{12}$. The theorem then comes down to showing that $|X_0(\ell)(\mathbb{F}_q)|$ is approximately $\frac{\ell+1}{12}(\sqrt{q} - 1)$ when $q = p^2$. It is more generally true that $A(q) = \sqrt{q} - 1$ when q is a prime, but the proof is a little more complicated. Roughly, the modular curve $X_0(n)$ parametrizes (E, ϕ) where E is an elliptic curve and ϕ is an isogeny of degree n, or equivalently, an elliptic curve together with a cyclic subgroup of degree n. If $\ell \nmid p$ then $E[\ell](\overline{\mathbb{F}_p}) \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, which has $\ell + 1$ nonisomorphic cyclic subgroups of order ℓ.

One approach to proving this theorem is to show that a supersingular j-invariant defined over $\mathbb{F}_{p^2}$ gives rise to $(\ell + 1)$ rational points on $X_0(\ell)(\mathbb{F}_{p^2})$ points and then to count the number of such j-invariants. This is given in a rather elementary way in Chapter V of Silverman. We can first show that for a curve in Weierstrass form a curve $y^2 = f(x)$ being supersingular is equivalent to the x^{p-1} coefficient of $f(x)^{\frac{q-1}{2}}$ vanishing. This can be measured in terms of a certain polynomial $H_p(\lambda)$. By counting the degree of this polynomial and using some basic facts about elliptic curves, we can show that the number of supersingular j-invariants over $\mathbb{F}_{p^2}$ is approximately $\frac{p-1}{12}$. Putting this together completes the proof. A second approach is given by expressing $|X_0(\ell)(\mathbb{F}_q)|$ in terms of the trace of the qth Hecke operator acting on the space of cusp forms of weight 2 for $\Gamma_0(\ell)$. This approach shares some similarities with the use of the Selberg trace formula in Birch's theorem described a few lectures ago.

We then returned to discuss some main facts about elliptic curves over $\mathbb{C}$ that go into the proof of Deuring's theorem about $N(t)$. We stated some main facts about complex multiplication leading up to Deuring's lifting theorem, a major result which gives a connection between the endomorphism ring of an elliptic curve over a number field and the endomorphism ring of its reduction modulo prime ideals. We then used this result to give a detailed sketch of the proof of Deuring's theorem.

We did not have time to give full details about modular curves or about the proof of Deuring's theorem. There are lots of great resources for this. I would suggest looking at the last few lectures of Andrew Sutherland's Elliptic Curves course notes, the first section of Chapter 4 of Cox, or Moreno's book *Algebraic Curves over Finite Fields.*

22 Reading Period

During reading period we will have at least two additional presentations (and possibly more!) Please let me know if you would like to present so I can put a schedule together. I will continue updating a list of possible presentation topics that I think would work well.