Overview

Brian Conrad and Akshay Venkatesh [*]

September 30, 2015

1 Introduction to the BSD conjecture

1.1 Some history

The BSD conjecture originated from observations made by Birch and Swinnerton-Dyer when studying the asymptotics of

$$\prod_{p\leq x}\frac{\#E(\mathbf{F}_p)}{p}$$

as x grows ("the first serious contribution to mathematics by a computer"). Specifically, Birch and Swinnerton-Dyer found that

$$\boxed{\prod_{p\leq x}\frac{\#E(\mathbf{F}_p)}{p}\sim C_E(\log x)^{\mathrm{rank}(E(\mathbf{Q}))}}$$

for some (explicit) constant C_E. This phenomenon was then reformulated by Tate in terms of an L-function $L(E/\mathbf{Q},s)$ and then generalized to abelian varieties over global fields.

1.2 Motivation: the class number formula

Let me give a completely *ahistorical* motivation by going back to the zeta function.

If K is a number field, then it has an associated *Dedekind zeta function* ζ_K. One has that

$$\mathrm{ord}_{s=0}\,\zeta_K = r := r_1+r_2-1 = \mathrm{rank}(\mathcal{O}_K^\times).$$

Moreover, the leading coefficient C_K is described explicitly by fundamental invariants associated to K:

$$\boxed{C_K = -\frac{h_K R_K}{w_K}}$$

where

[*] Notes taken by Tony Feng

- h_K is the *class number* of K; i.e. the size of the class group $\mathrm{Pic}(\mathcal{O}_K) \simeq H^1_{\text{ét}}(\mathcal{O}_K, \mathbf{G}_m)$ (which classifies "$\mathbf{G}_m$-torsors over $\mathcal{O}_K$"),
- $w_K = \#(\mathcal{O}_K^\times)_{\text{tors}}$ is the number of roots of unity in K,
- R_K is the *regulator* of K, defined as follows. The map $\mathcal{L} \colon \mathcal{O}_K^\times \to \mathbf{R}^{r_1+r_2}$ is defined by

  $$\mathcal{L}(u) = (\log ||u||_v)_{v|\infty}$$

  (where complex places are taken in pairs, and for such places the norm used here is the square of the usual absolute value) and via the product formula this factors through the hyperplane $H = \{(t_i)_i \mid \sum t_i = 0\}$. There is a natural measure on H induced via the short exact sequence

  $$0 \to H \to \mathbf{R}^{r_1+r_2} \xrightarrow{\Sigma} \mathbf{R} \to 0$$

  and the Lebesgue measures on $\mathbf{R}^{r_1+r_2}$ and $\mathbf{R}$. (Explicitly, the measure on H corresponds to a choice of orthonormal basis via the standard inner product on $\mathbf{R}^{r_1+r_2}$.)

  Remark 1.2.1. It is a theme that comes up over and over again in number theory that when you have a short exact sequence

  $$1 \to H \to G \to G/H \to 1$$

  of locally compact Hausdorff topological groups and Haar measures chosen on two out of the three groups, then there is a unique choice of Haar measure on the third so that an appropriate "Fubini formula" holds among integration on the three spaces (characterized for integration of continuous functions with compact support, but valid and used in an L^1-sense too). This is discussed in Lang's book *Real and functional analysis* for the characterization aspect with continuous compactly-supported functions, and the L^1-aspect is then an instructive exercise.

  With respect to this preferred measure on H, we set $R_K = \mathrm{vol}(H/\mathcal{L}(\mathcal{O}_K^\times))$.

In Tate's reformulation of the BSD conjecture, there are analogous pieces to those appearing here. So the class number formula is a "$\mathbf{G}_m$-version over $\mathcal{O}_K$" of the BSD conjecture for the "Néron model over $\mathcal{O}_K$ for an abeian variety over K" (though the meaning and role and Néron models will be largely postponed until the next lecture, with ℓ-adic representations serving in place of Néron models today).

1.3 Construction of the L-function

Let A be an abelian variety over a global field K. We want to define an L-function $L(A/K, s)$.

The L-function will be constructed as an Euler product over local factors, which are related to the "reduction" of A at the primes of K. There are complications at places of bad reduction; some references on elliptic curves give case-wise formulas in these cases that may seem ad hoc without a broader context.

We shall give a *uniform* definition of the local factors of $L(A/K, s)$ using the (rational) *Tate module*

$$V_\ell(A) = T_\ell(A)[1/\ell],$$

which is a vector space isomorphic to $\mathbf{Q}_\ell^{2g}$, equipped with a continuous linear action of $\Gamma_K := \mathrm{Gal}(K_s/K)$.

Definition 1.3.1. Let R be a discrete valuation ring and X be a smooth proper scheme over $F := \mathrm{Frac}(R)$. We say that X has *good reduction* with respect to R if $X = \mathcal{X} \otimes_R F$ for some smooth proper R-scheme $\mathcal{X}$.

Hard facts. If A is an abelian variety, then A has good reduction at v (i.e. with respect to $\mathcal{O}_{K,v}$) if and only if A_{K_v} has good reduction with respect to $\mathcal{O}_{K,v}$. Moreover, in such cases we have $A = \mathcal{A}_v \otimes_{\mathcal{O}_{K,v}} K$ where $\mathcal{A}$ is an *abelian scheme* over $\mathcal{O}_{K,v}$ (i.e. a smooth proper $\mathcal{O}_{K,v}$-group scheme with connected reduction). In particular, the special fiber of $\mathcal{A}_v$ is an abelian variety over the residue field. This $\mathcal{A}_v$ is in fact *unique* and even *functorial* in A . All of these assertions rests crucially on the theory of Néron models, to be discussed next time.

Remark 1.3.2. This is really miraculous. For a general X with good reduction there is no preferred $\mathcal{X}$, but for *abelian varieties* there *is* is a preferred $\mathcal{X}$. Note that it isn't at all clear for general X that good reduction over the completion K_v should imply the same over K (i.e., relative to the algebraic localization $\mathcal{O}_{K,v}$).

If $\dim X = 1$ (and X is geometrically connected over F) with positive genus then there is a "best possible" $\mathcal{X}$ even when good reduction fails (the so-called minimal regular proper model, to be discussed later), but this lacks the good functoriality properties of the Néron model for abelian varieties.

If we want to make definitions (e.g. of the local factors of an L-function) for X in terms of an integral model $\mathcal{X}$, then it's not clear that this is independent of that choice. Beyond the case of curves and abelian varieties, there is no "best choice" of integral model:

Example 1.3.3. For a discrete valuation ring R with fraction field K and residue field k we shall give a smooth projective surface over K admitting two smooth projective R-models that are not R-isomorphic (even ignoring the chosen identification of their generic fibers).

The following example was suggested by R. Vakil. We will construct a projective smooth R-scheme $\mathcal{X}$ whose generic fiber is $\mathbf{P}^1_K \times \mathbf{P}^1_K$ and whose special fiber is the Hirzebruch surface $F_2 := \mathbf{P}(\mathcal{O} \oplus \mathcal{O}(2))$. (Note that $\mathbf{P}^1 \times \mathbf{P}^1$ may be viewed as the Hirzebruch surface F_0.) Then $\mathcal{X}$ and $\mathbf{P}^1_R \times \mathbf{P}^1_R$ have isomorphic generic fibers but non-isomorphic special fibers, so they are not R-isomorphic.

For the construction of $\mathcal{X}$, let $\mathcal{Q} \subset \mathbf{P}^3_R$ be the R-flat quadric $xy - z(z - tw) = 0$ where $t \in R$ is a uniformizer, so $\mathcal{Q}_K$ is smooth (hence the R-flat $\mathcal{Q}$ is reduced) and $\mathcal{Q}_k$ is a cone with singularity at $\xi_0 = [0, 0, 0, 1]$. Since $\mathcal{Q}_K$ is defined by a K-split quadratic form in 4 variables, namely $xy - zw'$ with $w' = z' - tw$, it is isomorphic to $\mathbf{P}^1_K \times \mathbf{P}^1_K$ (using $\mathbf{P}^1_K \times \mathbf{P}^1_K \hookrightarrow \mathbf{P}^3_K$ via $([\alpha, \beta], [u, v]) \mapsto [\beta u, \alpha v, \beta v, (\beta v - \alpha u)/t]$). Also, the blowup of the cone $\mathcal{Q}_k$ at the cone point ξ_0 is isomorphic to F_2.

Now we introduce an incidence relation over R that picks out one of the two lines through each point in $\mathcal{Q}_K$ by introducing an auxiliary slope parameter. Consider the closed subscheme $\mathcal{X} \subset \mathbf{P}^3 \times \mathbf{P}^1$ defined by

$$\{([x, y, z, w], [\alpha, \beta]) \,|\, \alpha x = \beta z, \beta y = \alpha(z - tw)\}$$

where $[\alpha, \beta]$ denotes homogeneous coordinates on $\mathbf{P}^1$. The projection $p_2 : \mathcal{X} \to \mathbf{P}^1$ is a $\mathbf{P}^1$-bundle: over $\{\beta \neq 0\}$ it is $\mathbf{P}^1$ with homogenous coordinates $[x, w]$ and over $\{\alpha \neq 0\}$ it is $\mathbf{P}^1$ with homogeneous coordinates $[y, w]$. Thus, $\mathcal{X}$ is R-smooth with geometrically connected fibers.

The projection $\mathcal{X} \to \mathbf{P}^3$ lands inside the quadric $\mathcal{Q}$ (as is sufficient to check over K since $\mathcal{X}$ is R-flat, or can be checked by working on fibers over $\operatorname{Spec}(R)$ since $\mathcal{Q}$ is reduced). The resulting map $\mathcal{X}_K \to Q_K = \mathbf{P}^1_K \times \mathbf{P}^1_K$ is an isomorphism since composing it with the first projection $\pi_1 : Q_K \to \mathbf{P}^1_K$ recovers the composite map $\mathcal{X}_K \hookrightarrow \mathbf{P}^3_K \times \mathbf{P}^1_K \to \mathbf{P}^1_K$ (as is sufficient to check in the sense of rational maps since $\mathcal{X}_K$ is integral); in other words, the smooth closed subscheme $\mathcal{X}_K \subset \mathcal{Q}_K \times \mathbf{P}^1_K$ lies inside the graph of π_1 and so must coincide with that graph.

The projection $\pi_1 : \mathcal{Q}_K \to \mathbf{P}^1_K$ extends to a map $\Pi_1 : \mathcal{Q} - \{\xi_0\} \to \mathbf{P}^1_R$ by using the two expressions $[y, z]$ and $[z - tw, x]$, so by the same reasoning as above we see that the inclusion $\mathcal{X} \subset \mathcal{Q} \times \mathbf{P}^1_R$ coincides with the graph of Π_1 away from $\{\xi_0\} \times \mathbf{P}^1_R = \mathbf{P}^1_k$. Hence, the projection $p_1 : \mathcal{X} \to \mathcal{Q}$ is an isomorphism over $\mathcal{Q} - \{\xi_0\}$, whereas $p_1^{-1}(\xi_0) \simeq \mathbf{P}^1_k$. Since $\mathcal{X}_k$ is a smooth surface, the curve $p_1^{-1}(\xi_0)$ is Cartier in $\mathcal{X}_k$. Hence, $(p_1)_k$ factors uniquely through the blow-up $\operatorname{Bl}_{\xi_0}(Q_k)$.

To prove that the unique $\mathcal{Q}_k$-map $f : \mathcal{X}_k \to \operatorname{Bl}_{\xi_0}(\mathcal{Q}_k) = F_2$ between smooth surfaces is an isomorphism, we have to show that the map $f_{\xi_0} : \mathbf{P}^1_k \to \mathbf{P}^1_k$ between ξ_0-fibers is an isomorphism. For this we shall go back to how a blow-up is built via charts. Direct computation over $\{w \neq 0\} = \mathbf{A}^3_k \subset \mathbf{P}^3_k$ shows that $\operatorname{Bl}_{\xi_0}(\mathcal{Q}_k)$ is covered by the charts $D_+(x)$ and $D_+(y)$, and the very definition of $\mathcal{X}_k = \mathcal{X} \bmod t$ identifies $D_+(x)$ with $\mathcal{X}_k \cap \{\beta \neq 0\}$ and identifies $D_+(y)$ with $\mathcal{X}_k \cap \{\alpha \neq 0\}$ compatibily with gluing data, so we are done.

In view of Example 1.3.3 we will make definitions in terms of the Galois representations intrinsically attached to the "generic fiber" X over K instead. This introduces a different problem, namely possible dependence on ℓ (and rationality issues to make sense of evaluating an ℓ-adic Euler factor on a complex number q_v^{-s}, but there are ways around this when we can link the Euler factor to a geometric object that doesn't involve ℓ (such as by using the Néron model in the case of abelian varieties, as we will see next time).

Remark 1.3.4. It is a soft fact that if R is a Dedekind domain and X is smooth and proper over $F = \mathrm{Frac}(R)$, then there exists $r \in R - \{0\}$ and a smooth proper $\mathcal{X}$ over $R[1/r]$ such that $X = \mathcal{X} \otimes_{R[1/r]} F$, so X has good reduction at all but finitely many maximal ideals of R. The principle is that any reasonable property over the (geometric) generic fiber "spreads out" to an open subset of $\mathrm{Spec}(R)$ (and this principle is valid with R any commutative ring whatsoever). There is an exhaustive discussion of this principle in EGA IV$_3$, §8–§9, §11, etc.

Let X be smooth and proper over a global field K, and $\ell \neq \mathrm{char}\,(K)$ be a prime. Then attached to X are étale cohomology groups $\mathrm{H}^i_{\text{ét}}(X_{K_s}, \mathbf{Q}_\ell)$, which are finite-dimensional $\mathbf{Q}_\ell$-vector spaces, equipped with a natural continuous Γ_K-action. (Here $X_{K_s} = X \otimes_K K_s$).

Example 1.3.5. If A is an abelian variey, then there is a Γ_K-equivariant isomorphism $\mathrm{H}^1_{\text{ét}}(A_{K_s}, \mathbf{Q}_\ell) \simeq V_\ell(A)^*$. The dual here means (as usual in representation theory) that the action of γ on $\mathrm{H}^1_{\text{ét}}(A_{K_s}, \mathbf{Q}_\ell)$ is identified with the linear dual of the action of γ^{-1} on $V_\ell(A)$.

Theorem 1.3.6. *If X has a smooth proper model $\mathcal{X}_v$ over $\mathcal{O}_{K,v}$ then $\mathrm{H}^i_{\acute{e}t}(X_{K_s}, \mathbf{Q}_\ell)$ is unramified at v, and naturally isomorphic to $\mathrm{H}^i_{\acute{e}t}(\mathcal{X}_v \otimes_{\mathcal{O}_{K,v}} \overline{\mathbf{F}}_v, \mathbf{Q}_\ell)$ as Galois modules with respect to the identification $D_v/I_v \simeq \Gamma_{\mathbf{F}_v}$.*

Remark 1.3.7. For abelian varieties, the *Néron-Ogg-Shafarevich criterion* provides a converse result (to be proved next time using Néron models). In general, there is no converse.

The upshot is that at unramified places, which constitute all but finitely many places, we have an action of Frobenius, so we can try to define an L-function following Artin's formalism for associating Artin L-functions to Galois representations: we consider the definition

$$L^i(X/K, s)\text{``}=\text{''}\prod_v \det(1 - q_v^{-s}\phi_v \mid (\mathrm{H}^i)^{I_v})^{-1}$$

where $q_v = \#\mathbf{F}_v$ and ϕ_v is the "geometric Frobenius" in D_v (inverse to the "classical Frobenius"). Strictly speaking, for the local factor at v we should require $\ell \neq \mathrm{char}(\mathbf{F}_v)$, as is automatic for global function fields but is a mild nuisance at the finitely many ℓ-adic places when K is a number field; we will address the resulting "independence of ℓ" issue shorrtly.

Remark 1.3.8. Why the geometric Frobenius rather than the classical one? The geometric Frobenius on cohomology is dual to the usual Frobenius on the Tate module in the case of degree-1 cohomology for abelian varieties. But the more serious reason stems from the Grothendieck-Lefschetz cohomological formula for L-functions attached to constructible ℓ-adic sheaves on separated schemes of finite type over finite fields, according to which the action of geometric rather arithmetic Frobenius in the Galois group is what appears.

To make sense of the putative definition of $L^i(X/K, s)$, there are some complications to be overcome:

1. The characteristic polynomial of ϕ_v on $(\mathrm{H}^i)^{I_v}$ lies a priori in $\mathbf{Q}_\ell[T]$, and thus seems to depend on ℓ. Moreover, it isn't clear what is meant by evaluating this ℓ-adic polynomial in a manner that involves q_v^{-s} with $s \in \mathbf{C}$. These concerns would be eliminated if the polynomial is actually in $\mathbf{Q}[T]$ and as such is independent of ℓ (with $\ell \neq \mathrm{char}(\mathbf{F}_v)$).

   One solution to this in practice, which is what we'll do for the abelian variety case, is to give a geometric re-interpretation which is evidently independent of ℓ. For abelian varieties, this goes through the Néron model (as we will explain next time, even for bad v). In general this is a serious issue, especially at the bad places. At places of good reduction it is settled using the Riemann Hypothesis proved by Deligne.

2. Does the product (absolutely) converge? To handle this we need to "uniformly" (in a power of q_v) bound the absolute values of the ϕ_v-eigenvalues in $\mathbf{C}$. The Riemann Hypothesis provides the bound, giving that $L(X/K, s)$ is absolutely convergent (uniformly in closed right half-planes) for $\mathrm{Rep}\, s > 1 + i/2$.

With the above issues settled, we can then consider analytic continuation, poles, leading terms, etc. This analytic continuation remains unsolved in general even for abelian varieties (though some cases are now known following the work of Wiles, Taylor, etc.).

This defines $L(A/K, s) = L^1(A/K, s)$ for $\mathrm{Re}(s) > 3/2$.

1.4 The BSD conjecture

First we discuss the "weak form".

Conjecture 1.4.1 (Weak BSD)**.** *$L(A/K, s)$ has analytic continuation to $\mathbf{C}$ and*

$$\mathrm{ord}_{s=1} L(A/K, s) = \mathrm{rank}\, A(K).$$

Evidence. Very little of the conjecture has been proven; there is progress for $\dim A = 1$ with "rank" (algebraic or analytic) ≤ 1 for some classes of K.

The best evidence (in B. Conrad's opinion) is for K a global function field and A the Jacobian of a curve. The point is that here one has an interpretation via surfaces over finite fields, called the *Artin-Tate conjecture.* To a curve over a global function field we can attach canonically a fibered surface over a finite field via the theory of minimal regular proper models, to be discussed later. The BSD conjecture for the Jacobian of such a curve is then equivalent to a conjecture about this surface which *makes sense for any smooth projective surface* over a finite field (in particular, having nothing to do with a fibration structure).

Now we discuss the "strong form" of the conjecture, which also predicts the leading coefficient.

Conjecture 1.4.2. *Near $s = 1$, we have*

$$L \sim C_A (s-1)^{\operatorname{rank} A(K)}$$

where

$$C_A = \frac{\# Ш_A \cdot R_A \cdot \Omega_A}{\# A(K)_{\mathrm{tors}} \cdot \# \widehat{A}(K)_{\mathrm{tors}}}.$$

We shall now briefly describe the various terms (with some details postponed to next time), and see how this is analogous to the class number formula.

- Here $Ш_A$ is the *Tate-Shafarevich group* of A. This admits a definition in terms of Galois cohomology, to be discussed later, and it is also closely related to the étale cohomology group $\mathrm{H}^1_{\text{ét}}(\mathcal{O}_K, \mathcal{A})$ for the Néron model $\mathcal{A}$ of A (analogous to the term $\mathrm{H}^1_{\text{ét}}(\mathcal{O}_K, \mathbf{G}_m)$ appearing in the class number formula). A precise definition will be given next time. This is the analogue of the class group. It is a major open problem to prove the finiteness of this group (known in some very special cases related to low-rank elliptic curves).

- The regulator is a volume term. There is a canonical height pairing

  $$A(K)_{\mathbf{R}} \times \widehat{A}(K)_{\mathbf{R}} \to \mathbf{R}$$

  and the volume is attached to the lattice $A(K) \times \widehat{A}(K) \hookrightarrow A(K)_{\mathbf{R}} \times \widehat{A}(K)_{\mathbf{R}}$ with respect to this pairing.

- Ω_A is a volume term involving the archimedean and bad places (encoding "Tamagawa factors").

Cassels discovered an interesting structure for elliptic curves, which was then generalized for abelian varieties by Tate, now known as the *Cassels-Tate pairing*:

$$\langle \cdot, \cdot \rangle_A : Ш_A \times Ш_{\widehat{A}} \to \mathbf{Q}/\mathbf{Z}.$$

(Definitions of this will be discussed later.) The construction shows that this is skew-symmetric with respect to double-duality. If $\phi \colon A \to \widehat{A}$ is a polarization (which, roughly speaking, is a symmetric isogeny to the dual abelian variety satisfying a positivity property) then inserting it into the second variable yields (by symmetry of ϕ) a skew-symmetric form on $Ш_A$.

A serious result concerning the Cassels–Tate pairing is that the kernel on each side of the pairing coincides with the maximal divisible subgroup $(Ш_A)_{\mathrm{div}}$. (Recall that an abelian group M is *divisible* if n-multiplication on M is surjective for all $n > 0$; e.g., $\mathbf{Q}_p/\mathbf{Z}_p$ is divisible for any prime p, as is $\mathbf{Q}/\mathbf{Z}$.) Thus, if ϕ is a *principal* polarization (i.e. $\deg \phi = 1$) then the resulting skew-symmetric form on $Ш_A/(Ш_A)_{\mathrm{div}}$ has trivial kernel in each variable; hence, the pairing is perfect if $Ш_A/(Ш_A)_{\mathrm{div}}$ is finite.

It is well-known that if X is a smooth projective geometrically connected curve over K then $A = \mathrm{Jac}(X)$ then A has a canonical principal polarization. A basic algebra fact is that given a finite abelian group with a perfect skew-symmetric form valued in $\mathbf{Q}/\mathbf{Z}$, the size of the odd part has to be a square (this is the analogue of the fact that a symplectic space has to have even dimension). The upshot is that if A admits a principal polarization, then the size of the odd part of $Ш/Ш_{\mathrm{div}}$ – if this group is finite! – is either a square or twice a square.

Given an ample line bundle $\mathcal{L}$, one get a polarization $\phi_{\mathcal{L}}$ in the usual manner (functorially defined by $x \mapsto t_x^*(\mathcal{L}) \otimes \mathcal{L}^{-1}$). However, for abelian varieties over general fields there are examples (when the ground field is not separably closed) of polarizations that do not come from this construction (which happens for $A = \mathrm{Jac}(X)$ and some curves X over number fields K with $X(K) = \emptyset$; recall that in such cases the principal polarization is built indirectly via Galois descent). Tate showed that if $\phi = \phi_{\mathcal{L}}$ for some $\mathcal{L}$ (as happens for elliptic curves, but generally not for the principal polarization of higher-genus curves without a rational point) then the associated perfect skew-symmetric form on $Ш_A$ is even *alternating*, so in such cases $\#Ш_A$ is a perfect square (even at 2).

Remark 1.4.3. Possibly due to a general lack of appreciation for the fact that *not* every polarization arises from a line bundle on A itself, there arose a folklore belief (never stated by Tate!) that for a principally polarized A, $\#Ш_A$ is a square. In 1999 Poonen and Stoll gave examples of Tate-Shafarevich groups of principally polarized Jacobians of higher-genus curves over $\mathbf{Q}$ whose order is not a square.

In fact they went much further: they discovered a 2-torsion cohomological invariant whose vanishing corresponds to the alternating property for a principally polarized abelian variety. Using this, they found another incredible example: a principally polarized Jacobian for which $\#Ш$ is a square but the Cassels-Tate form is *not* alternating!

1.5 Isogeny invariance

Since we can basically prove nothing, one might ask how to test it - e.g. if there are ways of probing whether or not the formulation is good with respect to known properties of L-functions.

The L-function is built out of the ℓ-adic representations, which are evidently invariant under isogeny. More precisely, if $f\colon A \to B$ is an isogeny then $V_\ell(A) \simeq V_\ell(B)$, so $L(A/K, s) = L(B/K, s)$. For the conjecture to be true, we must then have $C_A = C_B$. Recall that

$$C_A = \frac{\#Ш_A \cdot R_A \cdot \Omega_A}{\#A(K)_{\mathrm{tors}} \cdot \#\widehat{A}(K)_{\mathrm{tors}}}.$$

In general torsion isn't isogeny-invariant, and $\#Ш$ likewise is not (it is essentially an "integral" cohomology group). Overall, none of the pieces going into the definition of C_A are invariant under isogeny. However, it turns out that the combination C_A *is* isogeny invariant. This is a theorem of Tate, which will be discussed later in the seminar for number fields (see Theorem 7.3 in Chapter I of Milne's book *Arithmetic Duality Theorems*, which uses the full force of Tate global duality to be discussed in a couple of weeks, along with the Cassels–Tate pairing).

A serious issue with the BSD conjecture, noted above, is that it's not even known that $\#Ш_A < \infty$. What is known is a much more elementary result that $Ш_A[m]$ is finite for any $m > 0$ not divisible by $\mathrm{char}\,(K)$ (as will follow immediately from general finiteness theorems in global Galois cohomology to be discussed in a couple of weeks; see Remark 6.7 in Chapter I of Milne's book *Arithmetic Duality Theorems*); the same holds if $\mathrm{char}\,(K)|m$ but requires deeper methods with group schemes and flat cohomology.

Of course, the m-torsion finiteness for all $m > 0$ isn't good enough to prove the finiteness of $Ш_A$, since we haven't ruled out possibilities such as that perhaps $Ш_A \supset \mathbf{Q}_7/\mathbf{Z}_7$: the group $\mathbf{Q}_7/\mathbf{Z}_7$ has finite m-torsion for any $m > 0$, but is obviously infinite. (This is an instance of a "divisible group": an abelian group on which n-multiplication is surjective for every integer $n > 0$.) However, it is a formal consequence of finiteness of the ℓ-torsion finiteness for a prime ℓ that the ℓ-primary part of the torsion abelian group $Ш_A/(Ш_A)_{\mathrm{div}}$ (the quotient by the maximal divisible subgroup) is finite:

Lemma 1.5.1. *Let M be an abelian group that is ℓ-power torsion for a prime ℓ. If $M[\ell]$ is finite then M/M_{div} is finite.*

Proof. By the snake lemma applied to the ℓ-power endomorphism of the exact sequence

$$0 \to M_{\mathrm{div}} \to M \to M/M_{\mathrm{div}} \to 0$$

we see that $M[\ell] \to (M/M_{\mathrm{div}})[\ell]$ is surjective. Hence, we may replace M with M/M_{div} to reduce to the case that $M_{\mathrm{div}} = 0$ (it is a simple exercise that M/M_{div} has vanishing maximal divisible subgroup). In other words, the descending sequence of subgroups $\ell^n M$ has vanishing intersection.

Our aim now is to show that M is finite. By Pontryagin duality, it is equivalent to prove finiteness for the compact Hausdorff abelian dual M' of M. This dual is a pro-ℓ group (dual to M being ℓ-power torsion), and the maximal subgroup $M_{\mathrm{div}} \subset M$ on which ℓ-multiplication is surjective is dual to the "smallest" torsion-free quotient of M'; i.e., M_{div} is dual to M'/M'_{tor}. Hence, M' is torsion. Likewise, $M[\ell]$ is dual to $M'/\ell M'$, so $M'/\ell M'$ is finite. By compactness of M', if we choose $m'_1, \dots, m'_d \in M'$ representing generators of $M'/\ell M'$ then the natural map

$$\mathbf{Z}_\ell^d \to M'$$

defined by $(a_j) \mapsto \sum a_j m'_j$ is surjective modulo ℓ and hence is surjective by successive approximation with pro-ℓ groups. Thus, the commutative pro-ℓ group M' is a finitely generated as a $\mathbf{Z}_\ell$-module. But M' is torsion, so it is clearly finite. □

In general we do not know for number fields K how to rule out the possibility that $Ш_A/(Ш_A)_{\mathrm{div}}$ has nontrivial ℓ-primary part for infinitely many primes ℓ. By contrast, in the function field case the situation is much better, as we'll soon see.

1.6 Artin-Tate conjecture

Suppose K is the function field of a smooth proper geometrically connected curve C over a finite field κ. Given a smooth proper and geometrically connected curve $X \to \operatorname{Spec} K$ of positive genus, there is a *minimal regular proper model* $\mathcal{X} \to C$. (Thus, $\mathcal{X}$ is a smooth proper and geometrically connected surface over $\mathbf{F}_q$; it is projective by construction.) There is a lot of interesting geometry associated to this surface (ignoring its fibration structure over C):

- the Néron-Severi group $NS(\mathcal{X})$, which has an intersection pairing; this is closely related to $J(K)$ equipped with its height pairing.
- Artin realized that $Ш_J$ is closely related to $\mathrm{Br}(\mathcal{X}) := \mathrm{H}^2_{\text{ét}}(\mathcal{X}, \mathbf{G}_m)$; e.g., the finiteness of each is equivaent to that of the form, and the Brauer group admits a pairing analogous to the Cassels–Tate pairing.
- The zeta function $\zeta_{\mathcal{X},\mathbf{F}_q}$ is closely related to $L(J/K, s)$.

$\mathcal{X}$	X
$NS(\mathcal{X})$	$J(X)$
$\mathrm{Br}(\mathcal{X})$	$Ш_J$
$\zeta_{\mathcal{X},\mathbf{F}_q}$	$L(J/K, s)$

Tate realized that one could recast the entire BSD conjecture for X in terms of the invariants on the $\mathcal{X}$-side. The L-function of J (in contrast with more general abelian varieties!) is known to have analytic continuation via the link to the zeta function of the surface, and Tate proved the following compelling result.

Theorem 1.6.1 (Tate)**.** *In the notation above, we have*

$$\operatorname{rank}_{s=1} L \geq \operatorname{rank} J(K).$$

Tate analyized a natural pairing built on $\mathrm{Br}(\mathcal{X})$ via étale cohomology, including perfectness and skew-symmetry properties, and deduced that if the order were finite then it must be a square or twice a square. Manin found examples where the size is $\mathbf{Z}/2\mathbf{Z}$. But 30 years later, a mistake was found in Manin's example, and it was proved that actually the order is *always* a square (when finite), contrary to the Poonen–Stoll examples over number fields. This is *used* in the proof of the equivalence of the Artin–Tate for $\mathcal{X}$ and the BSD Conjectures for Jacobians J over global function fields, as we will see later.

2 Introduction to the Bloch-Kato conjecture

2.1 Siegel's mass formula

Let's begin with an active learning exercise. Consider the equation

$$x^2 + y^2 + z^2 = N$$

for a squarefree positive integer N. How many integral solutions are there when $N = 10001$?

There were several guesses from the audience. The correct answer is 1920 (the closest guess was 901).

Here is one approach. The question is obviously related to the geometry of the sphere of radius $r = \sqrt{N = 10001} \approx 100$. The lattice points lying in a spherical shell within a distance 1 of this sphere will necessarily be solutions to the equation. We can approximate the number of such lattice points by the volume of the spherical shell consisting of (x, y, z) with $|x^2 + y^2 + z^2 - 10001| < 1/2$, which is $4\pi r^2$ times the thickness of the shell. Since $(r + \delta)^2 - r^2 \approx 2r\delta$, the thickness should be about $\frac{1}{2\sqrt{N}}$, so the volume of the shell is about $2\pi\sqrt{N} \approx 600$.

However, there are some congruence conditions on the possible values of a sum of three squares. For instance:

Example 2.1.1. Consider the prime 2. The squares in $\mathbf{Z}_2$ are characterized modulo 8, and $x^2 \bmod 8$ depends only on $x \bmod 4$. If we assume that x, y, z take values uniformly at random modulo 8 (or modulo 4), then the distribution of $x^2+y^2+z^2$ is determined modulo 8, but it is *not* uniform: the values $1, 2, 5, 6$ modulo 8 are taken $3/16$ of the time each, the value 3 modulo 8 is taken $1/8$ of the time, the values $0, 4$ modulo 8 are taken $1/16$ of the time each, and 7 modulo 8 is never attained.

To account for this disparity, we should multiply the volume estimate by the ratio $\frac{3/16}{1/8} = \frac{3}{2}$ for $N \equiv 1, 2, 5, 6 \bmod 8$ (such as for $N = 10001$) and $\frac{1/8}{1/8} = 1$ for $N \equiv 3 \bmod 8$ (and 0 for $N \equiv 7 \bmod 8$), leading to an initial correction of 900 for $N = 10001$. Yet this remains far from the correct count.

A systematic perspective on Example 2.1.1, incorporating congruential information at all primes in a unified manner, goes back to Hardy–Littlewood. The idea is that after approximating the number of integral solutions with a volume estimate, we should adjust by multiplying against p-adic densities measuring p-adic non-uniformities for all primes p.

Miraculously, Siegel's "mass formula" proves that for positive-definite integral quadratic forms *which are unique in their genus*, this always converges to exactly the correct count! Fortunately, $x^2 + y^2 + z^2$ is unique in its genus (first proved by Gauss via his reduction theory for ternary quadratic forms in *Disquisitiones Arithmeticae*). Siegel proved a more general result that computed a weighted sum of "representation counts" $\#\{\vec{x} \in \mathbf{Z}^m \mid q(\vec{x}) = N\}$ across all quadratic lattices q in a fixed positive-definite genus, with the count equal to a product of local densities at all places of $\mathbf{Q}$ (the archimedean density playing the role of the volume term above).

The p-adic density measures non-uniformity in the distribution of values of the quadratic form $Q := x^2 + y^2 + z^2$ as a function $\mathbf{Z}_p^3 \to \mathbf{Z}_p$ for primes p. Consider the ratio of volumes $\mathrm{vol}(Q^{-1}(U))/\mathrm{vol}(U)$ relative to the standard Haar measure on $\mathbf{Z}_p$ (assigning volume 1 to both $\mathbf{Z}_p^3$ and $\mathbf{Z}_p$) as U varies through ever-smaller open balls centered at N. Such volume considerations will provide a precise language for probabilistic reasoning.

If the values of Q were "uniformly distributed" in the p-adic sense then such ratios would get close to 1 as U gets small. So we want to study these ratios for small U centered at N. Taking $U = N + p^e\mathbf{Z}_p$ with $e \geq 1$, the volume ratio for U is

$$\frac{\#\{(x,y,z) \in (\mathbf{Z}/p^e\mathbf{Z})^3 \,|\, Q(x,y,z) \equiv N \bmod p^e\}p^{-3e}}{p^{-e}}; \tag{2.1.1}$$

we want to understand the behavior as e grows.

If $p \nmid 2N$ then the affine quadric $\{Q = N\} \subset \mathbf{A}^3$ is $\mathbf{Z}_p$-smooth, so every solution to $Q(x,y,z) \equiv N \bmod p^e$ lifts in $p^3/p = p^2$ ways to a solution mod p^{e+1} for all $e \geq 1$. Hence, for such p the ratio is always equal to the value for $e = 1$:

$$\frac{\#\{(x,y,z) \in \mathbf{F}_p^3 \,|\, Q(x,y,z) = N \bmod p\}}{p^2}. \tag{2.1.2}$$

We will show below that this ratio is $1 + \frac{\left(\frac{-N}{p}\right)}{p}$. These quadratic residue symbols for $N = 10001$ are positive for all the small primes $3, 5, 7, 11, 13$, causing an "excess" beyond 1 for such "correction factors". By accounting for these and the appropriate p-adic density factors for $p|2N$ as discussed below, computing with the first 20000 primes yields something like 1919.8 for the heuristic prediction of the count of solutions; much better than 900, and very close to the true count of 1920.

Now let's elaborate on the calculation of the p-adic density for *all* primes p. (The impatient reader may skip ahead to Theorem 2.1.3.)

Case I. First we complete the discussion for $p \nmid 2N$ by showing that (2.1.2) is equal to $1 + \frac{\left(\frac{-N}{p}\right)}{p}$, or in other words that the number of solutions in $\mathbf{F}_p^3$ to $x^2 + y^2 + z^2 \equiv N \bmod p$ is $p^2 + p\left(\frac{-N}{p}\right)$. We will establish this count for *any* integer N (regardless of whether or not p divides $2N$), assuming p is odd.

Let $\chi = \left(\frac{\cdot}{p}\right)$ denote the Legendre symbol modulo p. Since $a \in \mathbf{Z}/p\mathbf{Z}$ is a square in $1 + \chi(a)$ ways, the count of interest is equal to

$$\begin{aligned} &\sum_{a,b \in \mathbf{Z}/p\mathbf{Z}} (1+\chi(a))(1+\chi(b))(1+\chi(N-a-b)) \\ =& \sum_{a,b \in \mathbf{Z}/p\mathbf{Z}} 1 + \sum_{a,b \in \mathbf{Z}/p\mathbf{Z}} \chi(a)\chi(b)\chi(N-a-b) \end{aligned}$$

because the other character sums cancel. Therefore, it suffices to show that

$$\sum_{a,b\in\mathbf{Z}/p\mathbf{Z}} \chi(a)\chi(b)\chi(N-a-b) = p\chi(-N). \tag{2.1.3}$$

Lemma 2.1.2. *We have*

$$S_N := \sum_{a\in\mathbf{Z}/p\mathbf{Z}} \chi(a)\chi(N-a) = \begin{cases} \chi(-1)(p-1) & N\equiv 0 \pmod p \\ -\chi(-1) & N\not\equiv 0 \pmod p. \end{cases}$$

Proof. By the same reasoning as used in the preceding paragraph,

$$\#\{(a,b)\mid a^2+b^2\equiv N \pmod p\} = p+S_N.$$

The case $N=0$ is now trivial, so we now assume $N\neq 0$. Hence, the conic $u^2+v^2=N$ in $\mathbf{A}^2_{\mathbf{F}_p}$ has smooth projective closure (since p is odd). Furthermore, it has a rational point by the pigeonhole principle, because the two expressions a^2 and $N-b^2$ each take $\frac{p+1}{2}$ values modulo p as a,b range over $\mathbf{F}_p$, and hence must share at least one value. Therefore, the projectivization of the conic is isomorphic over $\mathbf{F}_p$ to $\mathbf{P}^1_{\mathbf{F}_p}$, hence has exactly $p+1$ solutions over $\mathbf{F}_p$.

To complete the proof, it only remains to count the number of rational points of the conic on the line at infinity. But this is evidently 0 if $\chi(-1)=-1$ and 2 otherwise, which can be written uniformly as $1+\chi(-1)$.

In conclusion, we have found that if $N\not\equiv 0 \pmod p$ then

$$\#\{(a,b)\mid a^2+b^2\equiv N \pmod p\} = p+1-(1+\chi(-1)) = p-\chi(-1)$$

which shows that $S_N=-\chi(-1)$ in this case, as desired. □

Rewriting (2.1.3) as

$$\sum_{b\in\mathbf{Z}/p\mathbf{Z}} \chi(b) \sum_{a\in\mathbf{Z}/p\mathbf{Z}} \chi(a)\chi(N-a-b) = \sum_{b\in\mathbf{Z}/p\mathbf{Z}} \chi(b)S_{N-b}$$

we can use Lemma 2.1.2 to simplify it to

$$\begin{aligned}\sum_{b\not\equiv N} -\chi(b)\chi(-1)+\chi(N)\chi(-1)(p-1) &= \sum_{b\in\mathbf{Z}/p\mathbf{Z}} -\chi(b)\chi(-1)+\chi(N)\chi(-1)p \\ &= \chi(-N)p\end{aligned}$$

as desired. This completes the determination of the p-adic density when $p\nmid 2N$.

Case II. What if $p=2$? In Example 2.1.1 we computed (2.1.1) for $p=2$ and $e=3$, getting the ratio $3/2$ for $N\equiv 1,2 \bmod 4$ and 1 for $N\equiv 3 \bmod 8$ (and the other cases either cannot occur for squarefree N or, as for 7 mod 8, admit no solutions at all). We claim that (2.1.1) for $p = 2$ stabilizes at all $e \geq 3$. If $x_0^2+y_0^2+z_0^2 \equiv N \bmod 2^e$ then for $e \geq 1$ we see that to solve

$$(x_0 + 2^e\epsilon_1)^2 + (y_0 + 2^e\epsilon_2)^2 + (z_0 + 2^e\epsilon_3)^2 \equiv N \bmod 2^{e+1}$$

the ϵ_j's drop out and so either the original triple is actually a solution modulo 2^{e+1} (in which case all 8 triples mod 2^{e+1} with the same reduction as (x_0, y_0, z_0) modulo 2^e are solutions modulo 2^{e+1}) or it does not lift to a solution modulo 2^{e+1}.

In cases when (x_0, y_0, z_0) is a solution mod 2^{e+1} then exactly half of the 8 classes mod 2^{e+1} sharing its reduction modulo 2^e will lift to solutions mod 2^{e+2}. Indeed, the congruence

$$(x_0 + 2^e\epsilon_1)^2 + (y_0 + 2^e\epsilon_2)^2 + (z_0 + 2^e\epsilon_3)^2 \equiv N \bmod 2^{e+2}$$

says exactly

$$x_0\epsilon_1 + y_0\epsilon_2 + z_0\epsilon_3 \equiv (N - x_0^2 - y_0^2 - z_0^2)/2^{e+1} \bmod 2.$$

The left side is a *nontrivial* linear form in the ϵ_j's because if x_0, y_0, z_0 all vanish mod 2 then N would be divisible by 4 (as we are assuming the triple is a solution modulo $2^{e+1} \in 4\mathbf{Z}$) yet N is assumed to be squarefree. Hence, exactly *half* of the 8 possibilities for $(\epsilon_1, \epsilon_2, \epsilon_3)$ mod 2 will work as claimed.

The upshot is that if we consider congruence classes of triples modulo $2^{e'}$ with $e' \geq 2$ (i.e., $e' = e + 1$ with $e \geq 1$) and consider them in 8-fold clumps based on reduction modulo $2^{e'-1}$ then half of each clump (i.e., 4 triples per clump) lifts to a solution modulo $2^{e'+1}$, with all 8 lifts of a triple providing solutions when any single one does. Hence, among all 64 lifts mod $2^{e'+1}$ of the 8 triples in such a clump of solutions mod $2^{e'}$, exactly half are solutions mod $2^{e'+1}$.

We have shown that if there are $\nu_{e'}$ solutions mod $2^{e'}$ then among the $8\nu_{e'}$ lifts of these to triples modulo $2^{e'+1}$ exactly $4\nu_{e'}$ of those lifts are solutions. In other words, $\nu_{e'+1} = 4\nu_{e'}$ for all $e' \geq 2$. This establishes the asserted stabilization of (2.1.1) for $p = 2$ and $e \geq 3$ (and actually for $e \geq 2$ if one does the computation for $e = 2$).

Case III. Finally, what about the p-adic density for an odd prime factor p of N? We claim that stabilization happens for $e \geq 2$. The key point is that any triple (x_0, y_0, z_0) that is a solution to the congruence modulo p^e with $e \geq 2$ cannot reduce to $(0, 0, 0)$ modulo p, as otherwise we would get $p^2|N$ since $e \geq 2$, contradicting that N is squarefree. Hence, lifting a solution moduloe p^e to a solution modulo p^{e+1} with $e \geq 2$ amounts to the congruence

$$(x_0 + p^e\epsilon_1)^2 + (y_0 + p^e\epsilon_2)^2 + (z_0 + p^e\epsilon_3)^2 \equiv N \bmod p^{e+1}$$

with unknown ϵ_j's that only matter modulo p and (x_0, y_0, z_0) that does not vanish modulo p. Since p is odd, this is exactly

$$x_0\epsilon_1 + y_0\epsilon_2 + z_0\epsilon_3 \equiv (1/2)(N - x_0^2 - y_0^2 - z_0^2) \bmod p$$

which is a *nontrivial* linear condition on the ϵ_j's. Thus, each solution modulo p^e lifts to p^2 solutions modulo p^{e+1} when $e \geq 2$, proving the asserted stabilization for odd $p|N$.

It remains to determine (2.1.1) for odd $p|N$ with $e = 2$. The preceding calculation for such p works equally well when $e = 1$ because we have already shown that any solution modulo p^2 must have *nonzero* reduction modulo p. Hence, if ν_e denotes the number of solutions modulo p^e then the absence of a mod-p^2 congruential solution lifting the solution $(0,0,0)$ to $x^2 + y^2 + z^2 \equiv N \bmod p$ implies $\nu_2 = p^2(\nu_1 - 1) = p^2(p^2 - 1)$, so

$$\frac{\nu_2}{p^4} = \frac{p^2 - 1}{p^2} = 1 - \frac{1}{p^2}.$$

Putting it all together, Siegel's theorem gives:

Theorem 2.1.3. *For a squarefree positive integer N,*

$$\#\{(x,y,z) \in \mathbf{Z}^3 \,|\, x^2 + y^2 + z^2 = N\} = 2\pi\sqrt{N}\rho_2 \cdot \prod_{p \nmid 2N} \left(1 + \frac{\psi(p)}{p}\right) \cdot \prod_{p | N_{\text{odd}}} (1 - 1/p^2),$$

where $\psi = \left(\frac{-N}{\bullet}\right)$ is the quadratic character associated to $\mathbf{Q}(\sqrt{-N})$ and the 2-adic density ρ_2 is equal to $3/2$ when $N \equiv 1, 2 \bmod 4$ and is equal to 1 when $N \equiv 3 \bmod 8$.

Remark 2.1.4. If N were permitted to have nontrivial square factors then the computations of the local densities at prime factors of N would change!

We want to relate this final expression to a Dirichlet L-function. For $p \nmid 2N$, we have

$$\left(1 + \frac{\psi(p)}{p}\right) = \left(1 - \frac{\psi(p)}{p}\right)^{-1} \left(1 - \frac{1}{p^2}\right) \tag{2.1.4}$$

as $\psi(p)^2 = 1$. For *odd* $p|N$, we have $\psi(p) = 0$ because p is ramified in $\mathbf{Q}(\sqrt{-N})$, so the factor $1 - 1/p^2$ at such p on the right side of Theorem 2.1.3 coincides with the right side of (2.1.4). Therefore, the count is equal to

$$2\pi\sqrt{N}\rho_2 \cdot \prod_{p>2} \left(1 - \frac{\psi(p)}{p}\right)^{-1} \left(1 - \frac{1}{p^2}\right)$$

Writing $L^{(\ell)}$ for the L-function with the Euler factor at a prime ℓ removed, this can be rewritten as

$$2\pi\sqrt{N}\rho_2 \cdot L^{(2)}(1,\psi)/\zeta^{(2)}(2).$$

By the analytic class number formula (recalled in Example 2.2.3 below) and Euler's calculation of $\zeta(2)$, this is

$$2\pi\sqrt{N}\rho_2 \left(1 - \frac{\psi(2)}{2}\right) \frac{2\pi h}{w\sqrt{d_N}} \cdot \frac{6}{\pi^2} \left(1 - \frac{1}{4}\right)^{-1}$$

where w is the number of integral units in $\mathbf{Q}(\sqrt{-N})$, h is its class number, and d_N is the absolute discriminant $\mathbf{Q}(\sqrt{-N})$ (so $d_N = N$ if $N \equiv 3 \pmod 4$ and $d_N = 4N$ otherwise; likewise, $w = 2$ except when $N = 1, 3$). Cancelling factors of π^2, etc., the count is equal to

$$\frac{4}{3} \cdot \rho_2 \left(1 - \frac{\psi(2)}{2}\right) \frac{12h}{w/2} \sqrt{\frac{N}{d_N}}.$$

This is still ugly, but we shall now transform it into something very clean, by separately considering different cases for N mod 8.

If $N \equiv 1, 2 \pmod 4$ then $\psi(2) = 0$, $\rho_2 = 3/2$, and $\sqrt{N/d_N} = 1/2$, so ρ_2 cancels out and we get the formula

$$\frac{12h}{w/2}$$

for the original count (so $w/2 = 1$ when $N > 1$); this applies to $N = 10001$. As a reality check, this gives the correct count for $N = 1$ due to the presence of $w/2$ (which is equal to 2 when $N = 1$), as well as for $N = 5$ (with $h = 2$).

If $N \equiv 3 \pmod 8$ then $\psi(2) = -1$, $\rho_2 = 1$, and $\sqrt{N/d_N} = 1$, so the count is

$$\frac{24h}{w/2}$$

(with $w/2 = 1$ when $N > 3$). As a reality check, this gives the correct count for $N = 3$ (with $w/2 = 3$) and $N = 11$ (with $h = 1$).

2.2 Hints of a general conjecture

Birch and Swinnerton-Dyer were inspired by Siegel's mass formula. Their idea was to estimate the size of $E(\mathbf{Q})$ using the product of "local densities" $\prod_{p \leq x} \frac{\#E(\mathbf{F}_p)}{p}$.

Remark 2.2.1. There is something subtle going on here. The Riemann Hypothesis for elliptic curves over finite fields suggests that it is more natural to compare $\#E(\mathbf{F}_p)$ to $p+1$ instead of p, yet such a change has a huge effect since $\prod_{p \leq x}(p+1)/p$ diverges like $\log x$.

For an elliptic curve $E/\mathbf{Q}$, Birch and Swinnerton-Dyer predict that

$$\frac{L^{(r)}(E, 1)}{r!} = \frac{Ш_E \cdot \Omega_E \cdot R_E}{E(\mathbf{Q})_{\text{tors}}^2}.$$

The goal of this year's learning seminar is to get to a generalization of this formula. For a variety X, you have cohomology groups $\mathrm{H}^i(X)$ and an L-function $L^i(X, s)$. We want to give a similar prediction for $L^i(X, q)$ at $q \in \mathbf{Z}$.

It is conjectured that this L-function has a functional equation relating the values at s and $i + 1 - s$. More precisely, a product of the form $L_\infty(s)L^i(X, s)$ is symmetric under $s \leftrightarrow i + 1 - s$. (The $L_\infty(s)$ should essentially be comprised of Gamma functions).

Let $\boxed{p = i + 1}$ and $\boxed{q^* = p - q}$. Without loss of generality, we may assume that $q \geq p/2$ and $q^* \leq p/2$. We briefly survey some of the evidence for such a conjecture.

Example 2.2.2. (*BSD conjecture.*) If $X = E$, then $i = 1$ and $p = 2, q = 1$. The Tate-Shafarevich group should be interpreted as a "generalized class number". The R_E is the size of a "generalized unit group" (analogous to the classical regulator). The Ω_E is, up to Tamagawa factors, $\int_{E(\mathbf{R})} \omega$ where ω is a rational form. We'll call it a "period" since it's the integral of an algebraic differential form over a cycle.

Example 2.2.3. (*The class number formula.*) Consider $\mathbf{Q}(\sqrt{d})$. There is an associated Dirichlet character χ_d, and

$$\zeta_{\mathbf{Q}(\sqrt{d})} = \zeta(s)L(s, \chi_d).$$

Then the class number formula says that

$$L(1, \chi_d) = \begin{cases} \frac{2\pi h}{w\sqrt{|d|}} & d < 0, \\ \frac{2hR}{w\sqrt{d}} & d > 0. \end{cases}$$

Here h is the class number and $2\pi/\sqrt{|d|}$ is like a period (coming from integrating over a circle). For $d < 0$ the formula involves a class number and a period, but no units. In the $d > 0$ case, there is a class number and units, but no period.

Writing in terms of the value at $s = 0$ instead, we get

$$L(0, \chi_d) = \zeta_{\mathbf{Q}(\sqrt{d})}(0)/\zeta_{\mathbf{Q}}(0) = \frac{2hR}{w}$$

(where h, R, and w are the usual invariants for $\mathbf{Q}(\sqrt{d})$).

Example 2.2.4. Another piece of evidence comes from the L-functions of modular forms. (Zagier attributes this to Eichler-Shimura-Manin.) The following type of statement was known by the early 70s. Let $\Delta = q\prod(1 - q^n)^{24} \in \mathcal{S}_{12}(1)$, so

$$\Delta = \sum \tau(n)q^n$$

and

$$L(\Delta, s) = \sum \frac{\tau(n)}{n^s}.$$

A fact about this is that there exist Ω_{even} and $\Omega_{odd} \in R$ such that

$$\frac{L(\Delta, q)}{(2\pi i)^q \Omega_q} \in \mathbf{Q}^*$$

for $1 \leq q \leq 11$. (Here $\Omega_q = \Omega_{even}$ if q is even and similarly if q is odd.) Two striking features of this are that there is a restricted range, and that there is a parity consideration.

Example 2.2.5. There are examples coming from other L-functions.

- Euler knew that $\zeta(2n) \in \mathbf{Q}\pi^{2n}$ and $\zeta(1-2n) \in \mathbf{Q}$.
- Hurwitz showed that

$$\sum_{(a,b)} \frac{1}{(a+bi)^{4n}} \in \mathbf{Q}\omega^{4n}, \quad \omega = \int_0^1 \frac{dx}{\sqrt{1-x^4}}.$$

2.3 Deligne's conjecture

In the end we'll have a precise conjecture, but for now we work up to $\mathbf{Q}^*$, which means that we can ignore class numbers. Deligne made a conjecture that describes examples with no regulator, i.e. no "unit group".

First, what does it mean to have "no unit group"? Deligne calls $L^i(X,q)$ is a *critical value* if $L_\infty(q) \neq \infty$ and $L_\infty(q^*) \neq \infty$. Deligne's conjecture is that

$$\boxed{L^i(X,q^*) \in \mathbf{Q}(2\pi i)^{1-q} \det\langle \omega_i, \gamma_j\rangle}$$

where ω_i is a $\mathbf{Q}$-basis for $F^q \mathrm{H}^i_{dR}(X)$ and γ_j is a $\mathbf{Q}$-basis for $H_{sing}(X(\mathbf{C}),\mathbf{Q})^{\pm}$. What does the $\pm$ mean? In BSD, you integrate ω against the real points of $E(\mathbf{R})$, so the complex conjugation comes into play. Here, the space $\pm$ is the $(-1)^{q-1}$ eigenspace for complex conjugation.

The fact that these two things have the same dimension is a consequence of the "criticality." In the case of an elliptic curve, this picks out the *holomorphic* differential and the *real* points of the elliptic curve.

What's going on in Example 2.2.4? In these terms, the point is that the Hodge structure has huge gaps. The 1 and 11 correspond to when the Hodge filtration changes. The reason why a parity condition enters is obvious.