BSD AND L-FUNCTIONS

1. Lecture 1: Review of arithmetic of elliptic curves

In this lecture we give a review of the basic arithmetic of elliptic curves. Proofs and more details of (almost) everything in this lecture can be found in Silverman's book [?MR2514094].

1.1. Definition of an elliptic curve.

Definition 1.1. An elliptic curve over a field k is a (smooth, proper, geometrically connected) curve of genus 1, equipped with a specified k-rational point O.

Over any field, any elliptic curve E may be given by a Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in k$ (more precisely, E is isomorphic to the curve in $\mathbb{P}^2$ given by homogenizing the above affine equation, with the point O being mapped to the unique point on the line at infinity). The condition that such an equation is smooth is that the *discriminant* $\Delta(a_1, ..., a_6)$ is non-zero. If the characteristic of k is different from $2, 3$ then one may in fact find an equation of the form

$$y^2 = x^3 + Ax + B$$

(for $A, B \in k$) and then we have $\Delta = -16(4A^3 + 27B^2)$.

The set of k-rational points $E(k)$ (or $E(\bar{k})$ for that matter) naturally form a group (either via the classical chord-tangent process or, equivalently, by checking that $P \mapsto (P) - (O)$ is a bijection between $E(k)$ and $\mathrm{Pic}^0(E/k)$) making E into a group variety.

Since E has genus 1 there is, up to scaling, a unique regular differential on E. It is given by

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

It is invariant under the group law in the sense that for any $P \in E(\bar{k})$, pull back along translation by P leaves ω invariant.

1.2. Elliptic curves over $\mathbb{C}$.

Let $\Lambda \subseteq \mathbb{C}$ be a lattice. For an integer $k \geq 2$ we define

$$G_{2k}(\Lambda) = \sum_{0 \neq w \in \Lambda} \frac{1}{w^{2k}}$$

which is absolutely convergent. We also define

$$g_2(\Lambda) = 60G_4(\Lambda) \text{ and } g_3(\Lambda) = 140G_6(\Lambda).$$

Let

$$E : y^2 = x^3 + Ax + B$$

be an elliptic curve over $\mathbb{C}$. Then there is a unique lattice $\Lambda \subseteq \mathbb{C}$ with $g_2(\Lambda) = -4A$ and $g_3(\Lambda) = -4B$. The map

$$\psi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$

given by

$$z \mapsto \left(\wp(z;\Lambda), \frac{1}{2}\wp'(z;\Lambda)\right)$$

is an isomorphism of complex Lie groups, where $\wp(z;\Lambda)$ is the Weierstrass $\wp$-function and $\wp'(z;\Lambda)$ its derivative. Moreover, we have $dz = \psi^*(\frac{dx}{2y})$.

Setting $\omega = \frac{dx}{2y}$ we may recover Λ as

$$\Lambda = \left\{ \int_\gamma \omega \;\mid\; \gamma \in H_1(E,\mathbb{Z}) \right\}.$$

We refer to this as the *period lattice* of E (which, of course, depends on our choice of ω).

The inverse of ψ is the map

$$P \mapsto \int_O^P \omega$$

where we note that this integral is well defined (i.e. path independent) modulo Λ.

For a fixed global 1-form ω on $E(\mathbb{C})$ the *complex period* is defined as

$$P_\omega = \frac{1}{2}\int_{E(\mathbb{C})} \mid \omega \wedge \bar{\omega} \mid .$$

If we take $\omega = \frac{dx}{2y}$ then we have

$$P_\omega = \frac{1}{2}\int_{\mathbb{C}/\Lambda} \mid dz \wedge \bar{dz} \mid = \int_{\mathbb{C}/\Lambda} dxdy$$

is just the area of the fundamental parallellogram of Λ.

1.3. **Elliptic curves over the reals.** Let E be an elliptic curve over the reals with Weierstrass equation $E : y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{R}$ so that $E(\mathbb{R})$ is a 1-dimensional real manifold. Let Λ be the associated period lattice. One sees easily that Λ is stable under the action of complex conjugation, and that the isomorphism $\psi : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ commutes with complex conjugation and defines an isomorphism of real Lie groups between $E(\mathbb{R})$ and the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-invariants of $\mathbb{C}/\Lambda$. Now complex conjugation σ acts on Λ as a matrix of order 2 in $\mathrm{GL}_2(\mathbb{Z})$. Since Λ is a lattice it cannot be contained in $\mathbb{R}$ or $i\mathbb{R}$, thus σ cannot be ± 1. Thus σ has eigenvalues 1 and -1 and one sees easily that we may find a basis ω_1, ω_2 for Λ on which σ acts as one of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In the first case, we see that Λ is generated by a positive real number w_{re} and a purely imaginary number w_{im}. Then $E(\mathbb{R})$ (inside $\mathbb{C}/\Lambda$) consists of the horizontal lines

$\mathrm{Im}(z) = 0$ and $\mathrm{Im}(z) = \frac{w_{\mathrm{im}}}{2}$. Thus $E(\mathbb{R})$ has 2-connected components and

$$\int_{E(\mathbb{R})} | \frac{dx}{2y} | = 2w_{\mathrm{re}}.$$

Moreover, in this case we have $E(\mathbb{R})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. In particular, this occurs if and only if the discriminant of E is positive.

In the second case, we see that Λ is generated by a non-real number w and its complex conjugate $\bar{w}$. Then $E(\mathbb{R})$ is just the real axis and $\int_{E(\mathbb{R}} | \frac{dx}{2y} | = w + \bar{w}$. In this case we have $E(\mathbb{R})[2] \cong \mathbb{Z}/2\mathbb{Z}$. This occurs if and only if the discriminant of E is negative.

In each case, we have

$$\int_{E(\mathbb{R})} | \frac{dx}{2y} | = [E(\mathbb{R}) : E^0(\mathbb{R})]\Omega_+$$

where Ω_+ is the unique positive generator of $\Lambda \cap \mathbb{R} \cong \mathbb{Z}$, the so-called *real period* (we caution again that this depends on the choice of differential/Weierstrass equation).

1.4. **Elliptic curves over local fields.** Let K be a non-archimedean local field, normalised valuation v, ring of integers $\mathcal{O}_K$, uniformiser π_K, residue field k of order q. Let E/K an elliptic curve. A Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E is *integral* if $v(a_i) \geq 0$ for all i (i.e. if each a_i is integral). Such an equation is *minimal* if it is integral and among all such integral models, $v(\Delta)$ is minimal. Note that if the equation is integral and $v(\Delta) < 12$ then it is automatically minimal. We write Δ_{min} for the minimal discriminant of E/K, which is well defined up to units.

Definition 1.2. We define the *reduction* of E to be the (possibly singular) curve $\tilde{E}/k$ obtained by reducing modulo π_K the coefficients of a minimal equation for E. One sees easily that this is independent of the choice of minimal equation (up to isomorphism over k). Moreover, the *minimal differential*

$$\omega^o = \frac{dx}{2y + a_1x + a_3}$$

relative to a minimal Weierstrass equation is well defined modulo units in $\mathcal{O}_K$.

If $v(\Delta) = 0$ for a minimal Weierstrass equation then E is an elliptic curve over k (and conversely). Either way, one can check that the usual chord tangent process makes the set $\tilde{E}_{\mathrm{ns}}(k)$ of non-singular k-points on $\tilde{E}$ into a group.

We have the following possibilities:

- $\tilde{E}/k$ is an elliptic curve ($\Leftrightarrow v(\Delta_{\mathrm{min}}) = 0$),
- $\tilde{E}/k$ is a genus 0 curve with a node. In this case we say E/K has *multiplicative reduction*. We further say that E/K has *split* (resp. *non-split*) multiplicative reduction if the node is split (resp. non-split). We have

$$\tilde{E}_{ns}(k) \cong \begin{cases} k^\times & \text{split mult.} \\ k(\sqrt{u})^\times_{\mathrm{Norm}=1} & \text{non-split mult.} \end{cases}$$

where here $u \in k^\times \setminus k^{\times 2}$. Note that $\tilde{E}_{\mathrm{ns}}(k)$ has order $q-1$ in the first instance, and $q+1$ in the second,

- $\tilde{E}/k$ is a genus 0 curve with a cusp. In this case we say that E/K has *additive reduction*. We have
$$\tilde{E}_{\mathrm{ns}}(k) \cong k$$
which has order q.

We have a natural reduction map $E(K) \to \tilde{E}(k)$ defined as follows. Given $P = [x : y : z]$ on $E(K)$, we scale the coordinates of P so that all of x, y, z are integral, and at least one is a unit. We then define $\bar{P} = [\bar{x} : \bar{y} : \bar{z}] \in \tilde{E}(k)$, noting that this is well defined. One checks that this restricts to a homomorphism $E_0(K) \to \tilde{E}_{\mathrm{ns}}(k)$ (where by definition $E_0(K)$ is the preimage of $\tilde{E}_{\mathrm{ns}}(k)$ under reduction, and is a subgroup of $E(K)$). We have a short exact sequence
$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{\mathrm{ns}}(k) \to 0,$$
with $E_1(K)$ being defined by the sequence, and surjectivity on the right following from Hensel's lemma.

The quotient $E(K)/E_0(K)$ is a finite abelian group (by a compactness argument using the v-adic topology on $E(K)$) and we define the *Tamagawa number*
$$c(E/K) = |E(K)/E_0(K)|.$$

Note that this is 1 if E has good reduction. If E/K has split multiplicative reduction then we have $E(K)/E_0(K) \cong \mathbb{Z}/v(\Delta_{\mathrm{min}})\mathbb{Z}$. In general, the Tamagawa number (and indeed the full structure of $E(K)/E_0(K)$) may be computed using Tate's algorithm.

1.5. **The formal group of E/K.** We wish to study the group $E_1(K)$ of points on a minimal Weierstrass equation reducing to the point at infinity on $\tilde{E}$.

We first make a change of variables so we can see the point at infinity in an affine chart. Specifically, write $z = -\frac{x}{y}$ and $w = -\frac{1}{y}$ (i.e. apply the transformation $[x : y : z] \mapsto [-x : -z : y]$ of $\mathbb{P}^2$ which sends $[0 : 1 : 0]$ to $[0 : 0 : 1]$ and look at the affine chart where the right most co-ardinate is equal to 1). We obtain the affine equation
$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3$$
and at $(0,0)$ the function z is a uniformiser. Then in the completed local ring at $(0,0)$ we can write w as a power series in z (by successively substituting for w into the right hand side of the above equation).

We obtain
$$w(z) = z^3 + a_1 z^4 + (a_1^2 + a_2) z^5 + (a_1^3 + 2a_1 a_2 + a_3) z^6 + \ldots \in \mathbb{Z}[a_1, \ldots, a_6][[z]].$$

We can then express the coordinate functions x and y as Laurent power series in z and obtain
$$x(z) = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \ldots$$
and
$$y(z) = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z - \ldots$$

and the minimal differential has equation

$$\omega = (1 + a_1 z + (a_1^2 + a_2)z^2 + ...)dz.$$

Now a point $P = (x, y)$ reduces to O if and only if one of x and y are non-integral. The Weierstrass equation for E shows that this occurs if and only if both x and y are non-integral, in which case $z = -\frac{x}{y} \in \pi_K \mathcal{O}_K$. Now given $z \in \pi_K \mathcal{O}_K$, the power series for $x(z)$ and $y(z)$ converge to elements in K which by construction lie in $E_1(K)$. This in fact gives us a bijection

$$\pi_K \mathcal{O}_K \to E_1(K).$$

Moreover, we can use the group law on $E(K)$ to find a power series $\mathcal{F}(z_1, z_2) \in \mathbb{Z}[a_1, ..., a_6][[z_1, z_2]]$ giving the group law on $\pi_K \mathcal{O}_K$ via this bijection. We have

$$\mathcal{F}(z_1, z_2) = z_1 + z_2 + (2 - a_1)z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) + ...$$

This gives an example of a *formal group*. Now the group law on $\pi_K \mathcal{O}_K$ is determined by the power series $\mathcal{F}$ and since this starts $z_1 + z_2 + ...$, one sees that multiplication by n on $\pi_K \mathcal{O}_K$ is given by a power series whose leading term is nz. Using this, one proves the following important fact:

Lemma 1.3. *Multiplication by n is an isomorphism on $E_1(K)$ for all n coprime to the residue characteristic of K.*

Corollary 1.4. *If E/K has good reduction, then reduction gives an isomorphism*

$$E(K)[n] \cong \tilde{E}(k)[n]$$

for all n coprime to the residue characteristic of K.

1.6. **Periods at non-archimedean places.** Let ω^o be the minimal differential on E/K. Let $|\cdot|$ denote the absolute value on K normalised so that $|\pi_K| = \frac{1}{q}$.

Lemma 1.5. *We have*

$$\int_{E(K)} |\omega^o| = \frac{c(E/K)|\tilde{E}_{\mathrm{ns}}(k)|}{q}.$$

Sketch of proof. We first indicate what the left hand side means. The group $E(K)$ naturally has the structure of a K-analytic manifold of dimension 1. Let U be an open subset of $E(K)$ and $\psi : U \xrightarrow{\sim} V \subseteq_{\text{open}} K$ be a chart. Then the differential ω^o takes the form $f(z)dz$ on V where dz is the usual differential on K and $f(z)$ is a Laurent power series in z without poles in V. We then define

$$\int_U |\omega^o| = \int_V |f(z)| d\mu$$

where μ is the Haar measure on K normalised so that $\mathcal{O}_K$ has volume 1. We define the integral over $E(K)$ by glueing.

We now appply this to E/K. The subgroup $E_1(K)$ is open in $E(K)$ and (the inverse of) the map

$$z \mapsto (x(z), y(z))$$

coming from the formal group gives a chart

$$E_1(K) \xrightarrow{\sim} \pi_K \mathcal{O}_K \subseteq K$$

(though this is an isomorphism of groups only when we endow $\pi_K \mathcal{O}_K$ with the formal group law coming from E). Under this, the differential ω^o corresponds to

$$(1 + a_1 z + (a_1^2 + a_2) z^2 + ...) dz.$$

Now $1 + a_1 z + ...$ has absolute value 1 everywhere on $\pi \mathcal{O}_K$ so that

$$\int_{E_1(K)} |\omega^o| = \int_{\pi_K \mathcal{O}_K} d\mu = \frac{1}{q}.$$

Now since the differential ω^o is invariant, the resulting measure on $E(K)$ is a Haar measure, so that

$$\int_{E(K)} |\omega^o| = [E(K) : E_1(K)] \int_{E_1(K)} |\omega^o| = c(E/K) \frac{|\tilde{E}_{\mathrm{ns}}(k)|}{q}$$

as desired. □

Note that if ω is any differential on E then $\omega = \lambda \omega^o$ and we have

$$\int_{E(K)} |\omega| = |\lambda| c(E/K) \frac{|\tilde{E}_{\mathrm{ns}}(k)|}{q} = |\frac{\omega}{\omega^o}| c(E/K) \frac{|\tilde{E}_{\mathrm{ns}}(k)|}{q}$$

the last equality by definition.

1.7. **Elliptic curves over global fields.**

1.7.1. *Mordell–Weil theorem and heights.*

Theorem 1.6 (Mordell–Weil theorem)**.** *Let K be a global field and E/K an elliptic curve. Then the group $E(K)$ is finitely generated.*

The Mordell–Weil theorem says that $E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$ for some integer $r \geq 0$, where $E(K)_{\mathrm{tors}}$ is the (necessarily finite) torsion subgroup of $E(K)$. By definition, r is the *rank* of E/K, denoted $\mathrm{rk}(E/K)$. The question of how to determine the rank of a given elliptic curve will be discussed in more detail in Stoll's course.

There are two main ingredients in the proof of the Mordell–Weil theorem.

Step 1 (Weak Mordell–Weil theorem)**:** The group $E(k)/nE(k)$ is finite for some $n \geq 2$.

Step 2: Theory of heights.

The first step uses the theory of Selmer groups.

The precise input for the second step is the following:

Theorem 1.7. *Let K be a global field and E/K an elliptic curve. Then there is a symmetric bilinear pairing, the* canonical height pairing

$$\langle\ ,\ \rangle : E(K) \times E(K) \to \mathbb{R}$$

such that

(i) $\langle x, x\rangle \geq 0\ \forall x \in E(K)$ with equality if and only if $x \in E(K)_{\text{tors}}$,

(iii) *for each $M \geq 0$, the set*

$$\{P \in E(K)\ :\ \langle P, P\rangle \leq M\}$$

is finite.

Proof. (Sketch) Let M_K denote the set of places of K. We define for $P = [x_0 : ... : x_n] \in \mathbb{P}^n(K)$,

$$h(P) = \sum_{v \in M_K} \log\left(\max\{|x_0|_v, ..., \log|x_n|_v\}\right).$$

Now for an elliptic curve E/K, given by a Weierstrass equation, consider the x-coordinate map $x : E \to \mathbb{P}^1$. We define the *naive height* of a point $P \in E(K)$ as $h_0(P) = h(x(P))$, where $h(x(P))$ is defined using the above height function on $\mathbb{P}^1$. Note that this is (at least up to a constant which vanishes in the forthcoming limiting process) intrinsic to E since $\{1, x\}$ is a basis for $H^0(E, 2\mathcal{O})$.

We then define the *canonical height* of $P \in E(K)$ as

$$h(P) = \lim_{n\to\infty} \frac{1}{4^n} h_0(2^n P).$$

Then one shows that this is a quadratic form on $E(K)$ and that the associated bilinear pairing has the required properties. □

Exercise: Use the above theorem and finiteness of $E(K)/2E(K)$ to prove the Mordell–Weil theorem.

Definition 1.8. Let K be a global field and E/K an elliptic curve. The *regulator* of E/K is defined as the absolute value of the determinant of the height pairing:

$$\text{Reg}(E/K) = |\det\left(\langle P_i, P_j\rangle\right)_{i,j}|$$

where $\{P_i\}$ is any $\mathbb{Z}$-basis for $E(K)/E(K)_{\text{tors}}$.

1.7.2. *Computing the torsion subgroup.* Here we give an example of how the torsion subgroup of an elliptic curve may be computed in practice.

Consider the elliptic curve $E : y^2 = x^3 - 19x + 30$ over $\mathbb{Q}$. Its discriminant is $2^{10} \cdot 7^2$ hence it has good reduction over $\mathbb{Q}_p$ for $p \neq 2, 7$ and this equation is minimal at such primes. So for any odd prime $p \neq 7$, and n coprime to p, we have

$$E(\mathbb{Q})[n] \hookrightarrow E(\mathbb{Q}_p)[n] \cong \tilde{E}(\mathbb{F}_p)[n].$$

Taking $p = 3$ we have

$$\tilde{E}(\mathbb{F}_3) = \{\infty, (0,0), (1,0), (-1,0)\}$$

has order 4.

Taking $p = 5$ gives

$$\tilde{E}(\mathbb{F}_5) = \{\infty, (0,0), (2,0), (-2,0)\}$$

has order 4.

Combining the two statements above we see that $E(\mathbb{Q})_{\text{tors}}$ has order dividing 4, and since the points

$$\{\infty, (2,0), (3,0), (-5,0)\}$$

are in $E(\mathbb{Q})$ and generate a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ they consist of all the torsion points.

2. Lecture 2: Zeta functions, L-functions and BSD

2.1. **Zeta functions of schemes over finite fields.** Let $X/\mathbb{F}_q$ be a scheme of finite type. We define

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n\geq 1} |X(\mathbb{F}_{q^n})| \frac{T^n}{n}\right).$$

The *Zeta-function* of $X/\mathbb{F}_q$ is then the complex function defined by

$$\zeta(X, s) = Z(X/\mathbb{F}_q, q^{-s}).$$

One may check that this converges for $\mathrm{re}(s) > \dim(X)$.

Examples.

- Take $X = \mathbb{A}^1_{\mathbb{F}_q}$ so that $|X(\mathbb{F}_{q^n})| = q^n$. Then we have

$$\begin{aligned} Z(X, T) &= \exp\left(\sum_{n\geq 1} \frac{(qT)^n}{n}\right) \\ &= \exp\left(-\log(1 - qT)\right) \\ &= \frac{1}{1 - qT}. \end{aligned}$$

- Take $X = \mathrm{pt} = \mathrm{Spec}\mathbb{F}_q$. Then we have $|X(\mathbb{F}_{q^n})| = 1$ for all n. Then (analagously to the previous computation) we obtain

$$Z(X, T) = \frac{1}{1 - T}.$$

- Take $X = \mathrm{pt}$ of degree $r = \mathrm{Spec}\mathbb{F}_{q^r}$. Then we have

$$|X(\mathbb{F}_{q^r})| = \begin{cases} 0 & r \nmid n \\ r & r \mid n. \end{cases}$$

  Then one has

$$\begin{aligned} Z(X/\mathbb{F}_q, T) &= \exp\left(\sum_{n\geq 1} r \frac{T^{nr}}{nr}\right) \\ &= \frac{1}{1 - T^r}. \end{aligned}$$

Note that if X is (in a suitable sense) a disjoint union of schemes W and V then we have

$$Z(X, T) = Z(W, T)Z(V, T).$$

In particular, one can use the previous examples to deduce that

$$Z(\mathbb{P}^1_{\mathbb{F}_q}, T) = \frac{1}{(1 - T)(1 - qT)}.$$

In fact, although this is not totally obvious, one can also do this for countably infinite unions, so that in particular, one obtains, for any $X/\mathbb{F}_q$, the following Euler product expression

$$\begin{aligned} Z(X,T) &= \prod_{x \text{ closed pt of } X} Z(x,T) \\ &= \prod_{x \text{ closed pt of } X} \left(\frac{1}{1-T^{\deg x}}\right). \end{aligned}$$

2.2. **Weil conjectures.**

Theorem 2.1 (Weil conjectures)**.** *Let $X/\mathbb{F}_q$ be a smooth projective variety of dimension n. Then*

$$Z(X,T) = \frac{P_1(T)P_3(T)...P_{2n-1}(T)}{P_0(T)P_2(T)...P_{2n}(T)}$$

where the $P_i(T) \in \mathbb{Z}[T]$ are polynomials in T with $P_0(T) = 1-T$, $P_{2n}(T) = 1-q^nT$ and for each $1 \leq i \leq 2n$,

$$P_i(T) = \prod_j (1-\alpha_{ij}T)$$

for some algebraic integers α_{ij} having absolute value $q^{i/2}$ for each complex embedding (this last statement is referred to as the Riemann hypothesis).

Moreover, $Z(X,T)$ satisfies the functional equation

$$Z\left(X, \frac{1}{q^nT}\right) = \pm q^{n\chi/2}T^{\chi}Z(X,T)$$

where $\chi \in \mathbb{Z}$ is the Euler characteristic *of X.*

In fact, we have

$$P_i(T) = \det\left(1 - \mathrm{Frob}_q^{-1}T \;\middle|\; H^i_{\text{et}}(X, \mathbb{Q}_l)\right)$$

for any prime $l \nmid q$ (here $\mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is the arithmetic Frobenius, which acts on $\bar{\mathbb{F}}_q$ as $x \mapsto x^q$).

Example. Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$Z(X,T) = \frac{P_1(T)}{(1-T)(1-qT)}$$

where $P_1(T) = \det\left(1 - \mathrm{Frob}_q^{-1}T \;\middle|\; V_l(E)^{\vee}\right)$. Since $V_l(E)$ is a 2-dimensional $\mathbb{Q}_l$-vector space, $P_1(T)$ has degree 2, constant term 1 and leading coefficient q. The only possibility is that

$$Z(X,T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$$

where $a = q+1-|E(\mathbb{F}_q)|$.

It follows from the Riemann hypothesis that we have the *Hasse bound*

$$|a| \leq 2\sqrt{q}.$$

(Though this is very much overkill, there exists an elementary proof of this.)

2.3. **The L-function of an elliptic curve.** Let K be a global field and E/K an elliptic curve. For each place v of K, let $\tilde{E}/k_v$ be the reduced curve over the residue field. If E has good reduction at v, we define

$$L_v(E,T) = 1 - a_v T + q_v T^2$$

where $a_v = q_v + 1 - |\tilde{E}(k_v)|$.

For the places of bad reduction of E, we define

$$L_v(E,T) = \begin{cases} 1-T & E \text{ split mult at } v \\ 1+T & E \text{ non-split mult at } v \\ 1 & E \text{ additive at } v. \end{cases}$$

Definition 2.2. The L-function of E/K is defined as (the complex function)

$$L(E/K,s) = \prod_{v \text{ non-arch}} L_v(E, q_v^{-s})^{-1}.$$

The Hasse bound ensures that this converges absolutely for $\mathrm{Re}(s) > 3/2$.

Remark 2.3. From the example earlier, for places of good reduction we have

$$L_v(E,T) = Z(\tilde{E}/k_v, T)(1-T)(1-q_v T).$$

In fact, one checks easily that this formula holds for places of bad reduction too. One defines the *global zeta function* of E/K as

$$\zeta(E/K,s) = \prod_{v \text{ non-arch}} Z(\tilde{E}/k_v, q_v^{-s}).$$

By the above remark, we have

$$\zeta(E/K,s) = \zeta_K(s)\zeta_K(s-1)L(E/K,s)^{-1},$$

where here $\zeta_K(s)$ is the Dedekind–Zeta function of K. For $K = k(C)$ the function field of a smooth projective curve over a finite field k, we have

$$\zeta_K(s) = \zeta(C/k, s).$$

Remark 2.4. Note that at all places we have the important equality

$$L_v(E, q_v^{-1}) = \frac{|\tilde{E}_{\mathrm{ns}}(k_v)|}{q_v}.$$

2.4. **The completed L-function.** We now add in factors at archimedean places (in the number field case) and additional factors to simply the functional equation, to obtain the *completed L-function*.

2.4.1. *Number fields.* Let K be a number field and E/K and elliptic curve. Then the *completed L-function* is

$$\Lambda(E/K,s) = (\mathrm{Norm}(N(E/K))d_K^2)^{s/2} \left((2\pi)^{-s}\Gamma(s)\right)^{[K:\mathbb{Q}]} L(E/K,s)$$

where $N(E/K)$ is the *conductor* of E/K and d_K is the discriminant of K.

2.4.2. *Function fields.* Let K be a function field of genus g with field of constants $\mathbb{F}_q$ and E/K and elliptic curve. Then

$$\Lambda(E/K,s) = q^{\frac{s}{2}(\deg N(E/K)+4g-4)}L(E/K,s).$$

Conjecture 1 (Hasse–Weil conjecture)**.** *Let K be a global field and E/K an elliptic curve. Then the completed L-function $\Lambda(E/K,s)$ has a meromorphic continuation to the whole complex plane and satisfies the functional equation*

$$\Lambda(E/K,s) = w(E/K)\Lambda(E/K,2-s)$$

where $w(E/K) \in \{\pm 1\}$ is the global root number of E/K. Unless K is a function field and E/K a constant elliptic curve (i.e. has some Weierstrass equation with all coefficients in the field of constants), then $\Lambda(E/K,s)$ in fact has analytic continuation to the whole of $\mathbb{C}$.

This is known for all elliptic curves over K if either K is a function field, $K = \mathbb{Q}$ or K is a real quadratic field. Partial information is known over CM fields (see Thorne's course). The other main example is when E/K has (potential) complex multiplication, when again the conjecture is known to be true.

2.4.3. *Root numbers.* For a local field $\mathcal{K}$ and an elliptic curve $E/\mathcal{K}$, one may define its *local root number* $w(E/\mathcal{K}) \in \{\pm 1\}$. We shall not go into the details of this definition but we note that one has

$$w(E/\mathcal{K}) = \begin{cases} 1 & E \text{ has good or non-split multiplicative reduction} \\ -1 & E \text{ has split multiplicative reduction or } \mathcal{K} \text{ is archimedean} \end{cases}$$

with the case of additive reduction being more complicated but still computable in practice.

One then conjectures that when E is an elliptic curve over a global field K, denoting by M_K the set of places of K, that

$$w(E/K) = \prod_{v \in M_K} w(E/K_v).$$

This is known **(??)** in all the cases described above where the Hasse–Weil conjecture is known.

In particular, one expects the sign in the functional equation to be readily computable from local data.

2.5. **Statement of the Birch–Swinnerton-Dyer conjecture.** For this section, we refer to the Bourbaki article of Tate [?MR1610977] for more details.

Conjecture 2 (Birch and Swinnerton-Dyer conjecture part I)**.** *Let K be a global field and E/K an elliptic curve. Then we have*

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

Remark 2.5. Note that the order of vanishing of $L(E/K,s)$ agrees with the order of vanishing of the completed L-function $\Lambda(E/K,s)$.

Conjecture 3 (Birch and Swinnerton-Dyer conjecture part II)**.** *The leading term of the Taylor series of $L(E/K,s)$ at $s=1$ is given by*

$$\frac{1}{r!}L^{(r)}(E/K,s)\mid_{s=1}=\frac{\mathrm{Reg}(E/K)}{|E(K)_{\mathrm{tors}}|^2}|Ш(E/K)|\prod_{v|\infty}\int_{E(K_v)}|\omega|_v\cdot\prod_{v\nmid\infty}c(E/K_v)\left|\frac{\omega}{\omega_v^o}\right|_v$$

$$\cdot\begin{cases}\frac{2^{r_2}}{\sqrt{d_K}} & K \text{ number field}\\ \frac{1}{q^{g-1}} & K \text{ function field}\end{cases}$$

(here r is the order of vanishing at $s=1$ and r_2 is the number of complex places of K).

In what follows, we will refer to the right hand side of this formula as $\mathrm{BSD}(E/K)$.

For complex places v, one may, if one wishes, take as a definition

$$\int_{E(K_v)}|\omega|_v=\frac{1}{2}\int_{E(K_v)}|\omega\wedge\bar{\omega}|.$$

2.6. **Conceptualising BSD(E/K).** Here we aim to explain somewhat the terms that appear in part II of the Birch and Swinnerton–Dyer conjecture.

Let K be a fixed global field and E/K an elliptic curve. Fix a non-zero global differential ω. Combining Lemma 1.5 with Remark 2.4 gives, for each non-archimedean place v,

$$\int_{E(K_v)}|\omega|_v=c(E/K_v)\left|\frac{\omega}{\omega_v^o}\right|_v L_v(E,q_v^{-1}). \tag{2.6}$$

We'd like to say that the integral of $|\omega|$ over the Adelic points of E is simply equal to the product over all places of the left hand side of the above equation. However, this does not converge since the Euler product for the L-function does not converge for $s=1$. More specifically, for each place, let μ_v denote the measure on $E(K_v)$ induced by ω. We'd like to define a measure on the Adelic points of E by taking the product of these local measures. However, we again run into the problem that the L-function does not converge at $s=1$ when trying to do this. To salvage matters, we add in 'convergence factors'. That is, we take Haar measures

$$\mu_v'=\frac{1}{L_v(E,q_v^{-1})}\mu_v$$

at all non-archimedean places. Then $\prod_v\mu_v'(E(K_v))$ now does converge and we obtain a measure μ on $E(\mathbb{A}_K)$. This does not depend on the choice of differential due to the product formula and we have

$$\mu_v'(E(\mathbb{A}_K))=\prod_{v|\infty}\int_{E(K_v)}|\omega|_v\cdot\prod_{v\nmid\infty}c(E/K_v)\left|\frac{\omega}{\omega_v^o}\right|_v.$$

In fact, there is still a choice involved in this measure - we defined the local Haar measures with respect to a choice of additive Haar measure ν on K_v and specified their normalisations (this is not ideal since these normalisations behave badly under field extensions for example). It's more natural to start with an arbitrary Haar measure on

$\mathbb{A}_K$ and then use the induced Haar measures at each completion (which are well defined locally only up to scaling vanishing globally). If we divide the resulting Haar measure on $E(\mathbb{A}_K)$ by the value $\nu(\mathbb{A}_K/K)$ then we wind up eliminating the choice of ν. The resulting measure μ' on $E(\mathbb{A}_K)$ (the *Tamagawa measure*) satisfies

$$\mu'(E(\mathbb{A}_K)) = \prod_{v|\infty} \int_{E(K_v)} |\omega|_v \cdot \prod_{v\nmid\infty} c(E/K_v) \left|\frac{\omega}{\omega_v^o}\right|_v \cdot \begin{cases} \frac{2^{r_2}}{\sqrt{d_K}} & K \text{ number field} \\ \frac{1}{q^{g-1}} & K \text{ function field.} \end{cases}$$

Thus it makes sense to write

$$\mathrm{BSD}(E/K) = \frac{\mathrm{Reg}(E/K)}{|E(K)_{\mathrm{tors}}|^2} |Ш(E/K)| \mathrm{vol}(E(\mathbb{A}_K)).$$

In fact, given the presence of the L-function in the convergence factors, it is also natural to try and 'remove them' and define

$$\mathrm{Vol}(E(\mathbb{A}_K)) = \frac{\mu'_v(E(\mathbb{A}_K))}{\frac{1}{r!}L^{(r)}(E/K,s)}$$

instead (here we use the capital 'V' to distinguish from our previous definition of the volume). Then the second part of the Birch and Swinnerton–Dyer conjecture simply becomes

$$\frac{\mathrm{Reg}(E/K)}{|E(K)_{\mathrm{tors}}|^2}\mathrm{Vol}(E(\mathbb{A}_K)) = \frac{1}{|Ш(E/K)|}$$

which is reminiscent of a formula for the Tamagawa number of an algebraic torus. This idea was pushed further by Bloch [?MR570874] and lead eventually to the Bloch–Kato conjecture [?MR1086888], a vast generalisation of BSD (which also realises both BSD and the analytic class number formula as instances of the same conjecture).

2.7. **Known results.** (By no means intended to be comprehensive.)

Theorem 2.7 (Gross–Zagier [?MR833192], Kolyvagin [?MR954295])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with*

$$\mathrm{ord}_{s=1}L(E/\mathbb{Q},s) \leq 1.$$

Then

$$\mathrm{rk}(E/\mathbb{Q}) = \mathrm{ord}_{s=1}L(E/\mathbb{Q},s).$$

Moreover, $Ш(E/\mathbb{Q})$ is finite.

Remark 2.8. There is a generalisation of this result for modular elliptic curves over totally real fields due to Shouwu Zhang [?MR1826411]. The implication $\mathrm{rk}_{\mathrm{an}} = 0 \Rightarrow \mathrm{rk} = 0$ for CM curves over $\mathbb{Q}$ was earlier proven by Coates and Wiles [?MR0463176].

Under certain additional assumptions we have a partial converse to the above theorem due to Skinner, Urban and Wei Zhang in various combinations (see [?MR3148103], [?MR3295917] and the survey paper [?MR3307716]). We do not attempt to state precisely the conditions on $E/\mathbb{Q}$ for it to hold, but the conclusion is of the form

$$\mathrm{Sel}^p(E/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^r \quad \text{for } r \in \{0,1\}$$

for p odd implies that

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r.$$

Over a general number field the main result is the following (due to Cassels in this setting and generalised by Tate and Milne).

Theorem 2.9 ([?MR0179169], [?MR1610977], [?MR2261462, Theorem 7.3 and Remark 7.4])**.** *Let K be a global field and E/K an elliptic curve. Let E'/K be isogeneous to E (over K). Then $Ш(E/K)$ is finite if and only if $Ш(E'/K)$ is finite. Moreover, if this is the case then*

$$\mathrm{BSD}(E/K) = \mathrm{BSD}(E'/K).$$

Over function fields, much more is known and we will discuss this next lecture.

2.8. **The parity conjecture.** Assuming analytic continuation and functional equation of the L-function and considering the Taylor series about $s = 1$, one sees that

$$w(E/K) = (-1)^{\mathrm{ord}_{s=1} L(E/K,s)}.$$

In particular, a consequence of the Birch and Swinnerton-Dyer conjecture is the *parity conjecture*.

Conjecture 4 (Parity conjecture)**.** *Let K be a global field and E/K an elliptic curve. Then*

$$w(E/K) = (-1)^{\mathrm{rk}(E/K)}.$$

This is actually quite remarkable as it often gives a very simple way to predict that an elliptic curve has a rational point of infinite order.

Example 2.10. Let $E/\mathbb{Q}$ be the elliptic curve

$$E : y^2 + y = x^3 + x^2 - 10x + 10$$

which has Cremona label 123a1. The discriminant is $-41 \cdot 3^5$ and one easily checks that it has split multiplicative reduction at 3 and 41. Along with the real place, this gives

$$w(E/\mathbb{Q}) = (-1)^3 = -1$$

and hence the parity conjecture predicts that $\mathrm{rk}(E/\mathbb{Q})$ is odd, and hence positive. In fact, $P = (-4, 1)$ is a Mordell–Weil generator.

Remark 2.11. This sort of argument solves the congruent number problem for many values of n, conditional on the parity conjecture.

Theorem 2.12 ([?MR2831512, Theorem 1.2])**.** *Let K be a number field and E/K and elliptic curve. If $Ш(E/F)$ is finite for $F = K(E[2])$, then*

$$w(E/K) = (-1)^{\mathrm{rk}(E/K)}.$$

3. BSD over function fields

Here we analyse the Birch and Swinnerton-Dyer conjecture over function fields. Recall that for an elliptic curve E over a function field K, the L-function of E/K is known to have a meromorphic continuation to the whole of $\mathbb{C}$ and poles only when E is a constant elliptic curve. We have the following theorem.

Theorem 3.1 (Tate–Artin [?MR1610977], Milne [?MR0414558])**.** *Let K be a function field and E/K an elliptic curve. Then*

$$\mathrm{rk}E(K) \leq \mathrm{ord}_{s=1}L(E,s).$$

Moreover, we have equality if and only if $Ш(E/K)[l^\infty]$ is finite for any prime number l.

If this is the case, then the second part of the Birch and Swinnerton-Dyer conjecture also holds.

In this lecture we will sketch how to obtain meromorphic continuation of the L-function and the rank inequality from the Weil conjectures.

3.1. **Elliptic curves and elliptic surfaces.** Let k be a finite field and C/k a smooth projective, geometrically connected curve. Let $K = k(C)$.

Fix an elliptic curve E/K. For simplicity, we assume that E/K is not isotrivial (i.e. its j-invariant is non-constant).

Proposition 3.2. *There is a smooth, projective, geometrically irreducible surface $\mathcal{E}/k$ equipped with a surjective morphsim $\pi : \mathcal{E} \to C$ having generic fibre E. If we moreover assume that π is relatively minimal, then the pair $(\mathcal{E}, \pi)$ is unique.*

We do not prove this but illustrate the idea with the following example.

Example 3.3. Consider, for example, the elliptic curve

$$E : y^2 = x(x-t^2)(x-1) \ / \ \mathbb{F}_5(t).$$

Now the discriminant of the elliptic curve $y^2 = x(x-t^2)(x-1)$ is $16t^4(t-1)^2(t+1)^2$ so that the elliptic curve has good reduction away from $t = 0, \pm 1, \infty$. At $t = 0, \pm 1$ we have split multiplicative reduction and to check the reduction at $t = \infty$, let $x = t^2x', y = t^3y'$ and write $u = 1/t$, giving equation

$$y'^2 = x'(x'-1)(x'-u^2).$$

This equation is minimal at $u = 0$ and we see that we have split multiplicative reduction at $t = \infty$ also.

Now consider the surface over $\mathbb{F}_5$

$$\mathcal{E}_0 = \{y^2z - x(x-t^2z)(x-z) = 0\} \subseteq \mathbb{P}^2 \times \mathbb{A}^1$$

where x, y, z are variables on $\mathbb{P}^2$ and t is the variable on $\mathbb{A}^1$. We have a map $\pi_0 : \mathcal{E}_0 \to \mathbb{A}^1$ given by $([x : y : z], t) \mapsto t$. The fibre over any closed point x of $\mathbb{A}^1$ is a cubic curve over the residue field $\mathbb{F}_5(x)$. Thus we think of $\mathcal{E}_0$ as being a surface fibred in elliptic curves (save that at $t = 0, \pm 1$ the fibre is a nodal cubic curve).

Consider similarly the surface

$$\mathcal{E}_1 = \{y'^2z' - x'(x' - u^2z')(x' - z') = 0\} \subseteq \mathbb{P}^2 \times \mathbb{A}^1.$$

Again we have a natural map π_1 to $\mathbb{A}^1$ given by projecting onto the u coordinate.

The surfaces $\mathcal{E}_0$ and $\mathcal{E}_1$ glue along the change of variables $x = t^2x', y = t^3y', u = 1/t, z = z'$ to give a surface $\mathcal{E}_2$ which is now projective, and the maps π_0 and π_1 glue to give a morphism $\pi_2 : \mathcal{E}_2 \to \mathbb{P}^1$ which is surjective. Finally, we blow up (possibly multiple times) at the singular points of the surface, namely at $([x : y : z], t) \in \{([0 : 0 : 1], 0), ([1 : 0 : 1], \pm 1)\}$ and $([x' : y' : z'], u) = ([0 : 0 : 1], 0)$ to resolve the singularities and obtain a smooth projective surface $\mathcal{E}$ admitting a surjective morphism $\pi : \mathcal{E} \to \mathbb{P}^1$. Note that the map $t \mapsto ([0 : 1 : 0], t)$ defines a section σ to π.

Moreover, the generic fibre of $\mathcal{E} \to \mathbb{P}^1$ is simply our original elliptic curve E. In particular, the inclusion $k(\mathbb{P}^1) \hookrightarrow k(\mathcal{E})$ induced by π realises an isomorphism of $k(\mathcal{E})$ and $k(E)$ over $k(\mathbb{P}^1)$.

We now return to the general setting. As in the example above, the point O on $E(K)$ gives a section σ to π, whose image in $\mathcal{E}$ is isomorphic to C. We also refer to this curve as O.

3.2. **The L-function of an elliptic curve over a function field.** Let E/K be an elliptic curve over a function field $K = k(C)$ (constant field $k = \mathbb{F}_q$). Recall that we have defined, for each place v of K, a polynomial

$$L_v(E, T)$$

such that the L-function of E/K is given by

$$L(E/K, s) = \prod_{v \in M_K} L_v(E, q_v^{-s})^{-1}$$

where q_v is the order of the residue field at v. Note that (unlike the number field case) we have $q_v = q^{\deg v}$. It thus makes sense to define the formal power series

$$\mathcal{L}(E/K, T) = \prod_{v \in M_K} L_v(E, T^{\deg v})^{-1} \in \mathbb{Q}[[T]]$$

so that $L(E/K, s)$ is obtained from $\mathcal{L}(E/K, T)$ by setting $T = q^{-s}$.

Recall that for each place v, we have

$$L_v(E, T) = Z(\tilde{E}/k_v, T)(1 - T)(1 - q_vT).$$

Now let $\mathcal{E}/k$ be the associated elliptic surface. We have

$$\begin{aligned} Z(\mathcal{E}, T) &= \prod_{x \text{ closed pt of } C} Z(\mathcal{E}_x/\mathbb{F}_q, T) \\ &= \prod_{x \text{ closed pt of } C} Z\left(\mathcal{E}_x/k(x), T^{\deg(x)}\right). \end{aligned}$$

We observe that for a closed point x of C at which E has good reduction, we have

$$Z\left(\mathcal{E}_x/k(x), T^{\deg(x)}\right) = \frac{L_x(E, T^{\deg x})}{(1-T^{\deg x})(1-q_v T^{\deg x})} = \frac{L_x(E, T^{\deg x})}{(1-T^{\deg x})(1-(qT)^{\deg x})}.$$

Taking the product over all places gives

$$\mathcal{L}(E/K, T) = \frac{Z(C,T)Z(C,qT)}{Z(\mathcal{E},T)} \prod_{v \text{ bad}} Q_v(T)$$

where each $Q_v(T)$ is a rational function in T which may be determined by comparing the Zeta functions of the bad fibres of $\mathcal{E}$ with the corresponding local L-polynomials.

It now follows from the Weil conjectures that:

Theorem 3.4. *Let E be an elliptic curve over a function field K. Then $\mathcal{L}(E/K,T)$ is a rational function of T. In particular, $L(E/K,s)$ has a meromorphic continuation to the whole of $\mathbb{C}$.*

A careful case by case analysis of the $Q_v(T)$ above also proves:

Proposition 3.5. *Let K be a global function field and E/K an elliptic curve with associated elliptic surface $\mathcal{E}$. Then*

$$\mathrm{ord}_{s=1} L(E/K,s) = -\mathrm{ord}_{s=1}\zeta(\mathcal{E},s) - 2 - \sum_{v \text{ bad}} (m_v - 1)$$

where m_v is the number of irreducible components in the fibre of $\mathcal{E}$ at v.

Remark 3.6. Grothendieck's work [?MR1608788] on L-functions over function fields gives a much more refined analysis of the L-function which allows us to prove analytic continuation in the case where E is non-constant (and more besides).

3.3. **The Shioda–Tate formula.** In this section we relate rational points on E/K to divisors on the surface $\mathcal{E}$.

Let Γ be a prime divisor on $\mathcal{E}$ (=irred curve in $\mathcal{E}$). Consider the restriction $\pi|_\Gamma : \Gamma \to C$. There are two possibilities:

- $\pi(\Gamma) = \{\mathrm{pt}\}$: in this case we say that Γ is a *vertical* curve.
- $\pi(\Gamma) = C$: in this case we say that Γ is a *horizontal curve*. Associated to Γ is a valuation μ_Γ on $k(\mathcal{E}) = k(E)$. The assumption that Γ is horizontal means that μ_Γ is trivial on $k(C)$. In particular, μ_Γ corresponds to a closed point P_Γ on E. The residue field at this point is simply the function field of Γ, so that $\deg P_\Gamma = [k(\Gamma) : k(C)]$ is the degree of the morphism $\pi|_\Gamma$.

The above discussion allows us to define a homomorphism

$$\alpha : \mathrm{Div}(\mathcal{E}) \longrightarrow \mathrm{Div}^0(E)$$

given by setting, for a prime divisor Γ,

$$\alpha(\Gamma) = \begin{cases} (P_\Gamma) - [k(\Gamma):k(C)](O) & \Gamma \text{ horizontal} \\ 0 & \Gamma \text{ vertical,} \end{cases}$$

and extending linearly.

Theorem 3.7 (Shioda–Tate)**.** *The map α induces a short exact sequence*

$$0 \to \mathbb{Z}O \oplus \mathbb{Z}F \oplus \bigoplus_{\Gamma \in S} \mathbb{Z}\Gamma \longrightarrow \mathrm{NS}(\mathcal{E}_{\bar{k}}) \longrightarrow \mathrm{Pic}^0(E_{\bar{k}}) = E(\bar{k}K) \to 0$$

where here

- $\mathrm{NS}(\mathcal{E}_{\bar{k}}) = \mathrm{Pic}(\mathcal{E}_{\bar{k}})/\mathrm{Pic}^0(\mathcal{E}_{\bar{k}})$ *(='divisors modulo algebraic equivalence') is the* Néron–Severi group *of $\mathcal{E}_{\bar{k}}$,*
- *F is any fibre (= π^*(closed pt on $C_{\bar{k}}$))*
- *S is the set of vertical prime divisors not meeting O.*

In particular, taking $\mathrm{Gal}(\bar{k}/k)$*-invariants, we deduce the Shioda–Tate formula*

$$\mathrm{rk}NS(\mathcal{E}) = \mathrm{rk}E(K) + 2 + \sum_{v \text{ bad}} m_v - 1,$$

where for each place v of bad reduction for E, m_v denotes the number of irreducible components in the fibre over v, and the Néron–Severi group of $\mathcal{E}$ is defined as the image of $\mathrm{Div}(\mathcal{E})$ *in* $\mathrm{NS}(\mathcal{E}_{\bar{k}})$ *(using that k is finite one sees that this agrees with $NS(\mathcal{E}_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)}$).*

N.B. any two fibres are algebraically equivalent.

Sketch of proof. We work the whole time over $\bar{k}$ and to ease notation we drop the subscripts.

The argument relies on the existence of the *intersection pairing*

$$\mathrm{Div}(\mathcal{E}) \times \mathrm{Div}(\mathcal{E}) \to \mathbb{Z}$$

which descends to the Néron–Severi group. Roughly speaking, the intersection of two curves on $\mathcal{E}$ is, not too suprisingly, the number of points in which they intersect, counted with multiplicity (when the curves are distinct). One then shows that this is invariant under linear equivalence where this makes sense. The pairing in general may now be defined by moving the curves via linear equivalence until one can define their intersection in the previous way. We say that two divisors are *numerically equivalent* if they cannot be distinguished via the intersection pairing.

α descends to the Néron–Severi group: First note that it clearly descends to $\mathrm{Pic}(\mathcal{E})$, for if $D = \mathrm{div}_{\mathcal{E}}(f)$ then the image under α is $\mathrm{div}_E(f)$. The general argument is fairly involved and we omit the full details. The map $\pi : \mathcal{E} \to C$ induces a homomorphism $\pi^* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(\mathcal{E})$ and clearly we're done if we show it's an isomorphism. More geometrically we can view π^* as a homomorphsim of abelian varieties between $\mathrm{Pic}^0_{C/k}$ and $\mathrm{Pic}^0_{\mathcal{E}/k}$. The presence of the section $\sigma : C \to \mathcal{E}$ ensures that π^* is injective so we must show it is surjective. Since the map is injective it suffices to show that π^* is an isogeny of abelian varieties, i.e. we may check surjectivity up to a finite index subgroup. There is now a nice geometric argument due to Shioda [?MR1081832, Theorem 4.1], starting from the above observation, which relies on a careful analysis of the intersection pairing on $\mathcal{E}$. This is where we need to know that E is non-isotrivial.

Surjectivity on the right: Any divisor $D \in \mathrm{Pic}^0(E)$ is linearly equivalent to $(P) - r(O)$ for some $P \in E$ a point of degree r. Since this is equal to the image of $\{\bar{P}\}$ under α, the map $\alpha : \mathrm{Div}(\mathcal{E}) \to \mathrm{Pic}^0(E)$ is surjective.

Exactness in the middle: It's immediate from the definition of α that O, F and all $\Gamma \in S$ are in the kernel of α. For the converse, suppose that $[D] \in \mathrm{NS}(\mathcal{E})$ is such that $\alpha(D) = 0 \in \mathrm{Pic}^0(E)$. Say $\alpha(D) = \mathrm{div}(f)$ for $f \in K(E) = k(\mathcal{E})$. Then $D - (D \cdot F)O - \mathrm{div(f)}$ is a vertical divisor. In particular, D is algebraically equivalent to an element of $\mathbb{Z}O \oplus \mathbb{Z}F \oplus \bigoplus_{\Gamma \in S} \mathbb{Z}\Gamma$.

Injectivity on the left: If some element of $\mathbb{Z}O \oplus \mathbb{Z}F \oplus \bigoplus_{\Gamma \in S} \mathbb{Z}\Gamma$ were algebraically equivalent to zero, then it would be numerically equivalent to zero, but one checks easily that this is not the case. □

Remark 3.8. We have shown in the course of the proof that numerical equivalence and algebraic equivalence agree for non-isotrivial minimal elliptic surfaces.

3.4. **The Artin–Tate conjecture.** If we combine the two sections above, we see that the BSD rank formula for E is equivalent to the equality

$$\mathrm{rk}NS(\mathcal{E}) = -\mathrm{ord}_{s=1}\zeta(\mathcal{E}, s).$$

Since in theory this statement has nothing to do with elliptic curves, one can ask if it holds for general smooth projective surfaces. This leads to:

Conjecture 5 (Artin–Tate part I)**.** *Let k be a finite field and X/k be a smooth projective surface. Then we have*

$$\mathrm{rk}NS(X) = -\mathrm{ord}_{s=1}\zeta(X, s).$$

(The so called 'theorem of the base' ensures that $NS(X)$ is finitely generated.)

There is also a version of BSD part II for all smooth projective surfaces over finite fields. It can be shown to be equivalent to BSD for all abelian varieties over function fields. Stating the precise conjecture is too much of a departure from the course, but we have the following approximate dictionary between elliptic curves and elliptic surfaces in general (though one should caution that, like the rank formula, the terms in BSD and the terms in Artin–Tate do not line up exactly and there is some work to be done in proving their equivalence):

Elliptic curve $E/k(C)$	Elliptic surface $\pi : \mathcal{E} \to C$ over k
L-function of E	Zeta function of $\mathcal{E}$
Group of rational points	Néron–Severi group
Height pairing	Intersection pairing on $NS(\mathcal{E})$
Shafarevich–Tate group	Brauer group of $\mathcal{E}$

3.5. **(Extremely brief) sketch of rank inequality.** Here we give a very brief sketch of the rank inequality part of Theorem 3.1. In what follows we write $\bar{\mathcal{E}} = \mathcal{E} \times_k \bar{k}$.

Fix a prime $l \neq p = \mathrm{char}(k)$ and consider the short exact sequence (of sheaves on $\bar{\mathcal{E}}_{\mathrm{et}}$)

$$0 \longrightarrow \boldsymbol{\mu}_{l^n} \longrightarrow \mathbb{G}_m \xrightarrow{x \mapsto x^{l^n}} \mathbb{G}_m \longrightarrow 0.$$

This gives a long exact sequence for etale cohomology from which we extract the short exact sequence

$$0 \longrightarrow H^1(\bar{\mathcal{E}}, \mathbb{G}_m)/l^n H^1(\bar{\mathcal{E}}, \mathbb{G}_m) \longrightarrow H^2(\bar{\mathcal{E}}, \boldsymbol{\mu}_{l^n}) \longrightarrow H^2(\bar{\mathcal{E}}, \mathbb{G}_m)[l^n] \longrightarrow 0.$$

Now $H^1(\bar{\mathcal{E}}, \mathbb{G}_m)$ is simply the Picard group of $\bar{\mathcal{E}}$. Moreover, since we are working over an algebraically closed field, $\mathrm{Pic}^0(\bar{\mathcal{E}})$ is divisible so that

$$H^1(\bar{\mathcal{E}}, \mathbb{G}_m)/l^n H^1(\bar{\mathcal{E}}, \mathbb{G}_m) \cong NS(\bar{\mathcal{E}})/l^n NS(\bar{\mathcal{E}})$$

and by definition we have $H^2(\bar{\mathcal{E}}, \mathbb{G}_m) = \mathrm{Br}(\bar{\mathcal{E}})$.

Putting this into the above sequence and taking the inverse limit over n we get an injection

$$0 \longrightarrow NS(\bar{\mathcal{E}}) \otimes \mathbb{Z}_l \longrightarrow H^2_{\text{et}}(\bar{\mathcal{E}}, \mathbb{Z}_l(1)).$$

Let Frob_q denote the Frobenius element $x \mapsto x^q$ which is a topological generator of $\mathrm{Gal}(\bar{k}/k)$. Then taking $\mathrm{Gal}(\bar{k}/k)$-invariants we deduce an injection

$$0 \longrightarrow NS(\mathcal{E}) \otimes \mathbb{Z}_l \longrightarrow H^2_{\text{et}}(\bar{\mathcal{E}}, \mathbb{Z}_l)^{\mathrm{Frob}_q^{-1}=q}$$

and one can relate the cokernel to the Brauer group of $\mathcal{E}$.

We now recall that the Zeta function of $\mathcal{E}$ has the form

$$Z(\mathcal{E}, T) = \frac{P_1(T)P_3(T)}{P_0(T)P_2(T)P_4(T)}$$

where

$$P_i(T) = \det\left(1 - \mathrm{Frob}_q^{-1} T \;\middle|\; H^i_{\text{et}}(X, \mathbb{Q}_l)\right)$$

and by the Riemann hypothesis, we see that $-\mathrm{ord}_{s=1}\zeta(\mathcal{E}, s)$ is equal to the multiplicity of q as a root of the characteristic polynomial of (the geometric) Frobenius acting on $H^2_{\text{et}}(\bar{\mathcal{E}}, \mathbb{Q}_l)$. But the short exact sequence gives

$$\mathrm{rk} NS(\mathcal{E}) \leq \dim_{\mathbb{Q}_l} H^2_{\text{et}}(\bar{\mathcal{E}}, \mathbb{Q}_l)^{\mathrm{Frob}_q^{-1}=q} \leq -\mathrm{ord}_{s=1}\zeta(\mathcal{E}, s)$$

and we are done.

With more effort, one can show that each inequality is an equality if and only if the Brauer group of $\mathcal{E}$ is finite (equivalently, if and only if the Shafarevich–Tate group of E/K is finite).

4. Lecture 4: The story in higher dimensions

4.1. **Abelian varieties.** A good reference for the basic theory of abelian varieties (of which we review a very small amount below) is [?MR861974].

Definition 4.1. Let k be a field. An *abelian variety* over k is a geometrically integral, projective group variety over k.

Remark 4.2. Usually the definition has 'proper' in place of 'projective' and one shows that all abelian varieties in this sense possess an ample line bundle and are hence projective. One sees easily that properness forces the group law to be commutative.

Elliptic curves are one dimensional abelian varieties (and conversely). Our main source of higher dimensional examples is that of Jacobians. Given a (smooth, projective, geom connected) curve C/k of genus g, one can associate a g-dimensional abelian variety J, the *Jacobian* of C. One has $J(k) = \mathrm{Pic}^0(C_{k^{\mathrm{sep}}})^{\mathrm{Gal}(k^{\mathrm{sep}}/k)}$ functorially.

Given an abelian variety A/k, $\mathrm{Pic}^0(A/\bar{k})$ has a natural structure of abelian variety defined over k, the *dual abelian variety* of A, which we denote $A^\vee$. For Jacobians, we have a canonical isomorphism $A \cong A^\vee$ (more precisely we have a canonical *principal polarisation*).

Any abelian variety A of dimension d over a field k is necessarily smooth and its sheaf of differentials $\Omega^1_{A/k}$ is a free $\mathcal{O}_A$-module of rank d. In particular, $\Lambda^d\Omega^1(A/K)$ is free of rank 1 whence

$$H^0(A, \Lambda^d\Omega^1(A/K)) \cong k.$$

Thus as with elliptic curves, up to scaling there is a unique non-zero regular d-form on A, which can be shown to be translation invariant.

4.2. **Abelian varieties over global fields.** If K is a global field then as with elliptic curves, the group $A(K)$ is finitely generated, so we may talk about the rank of A/K, denoted $\mathrm{rk}(A/K)$. The proof is more or less the same, using the theory of Selmer groups and heights (the latter to be discussed shortly).

4.2.1. *The L-function.* Given an abelian variety A/K, a nonarchimedean place v and $l \neq \mathrm{char}(k_v)$, let $T_l(E)$ denote its l-adic Tate module

$$T_l(E) = \lim_{\leftarrow} A[n] \cong \mathbb{Z}_l^{2d}$$

and let $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, a $2d$-dimensional $\mathbb{Q}_l$-vector space with action of $G_{K_v} := \mathrm{Gal}({K_v}^{\mathrm{sep}}/K_v)$. We define the *local L-polynomial*

$$L_v(A, T) = \det\left(1 - \mathrm{Frob}_v^{-1} T | (V_l(A)^\vee)^{I_v}\right)$$

where here I_v denotes the inertia group at v, Frob_v is the (arithmetic) Frobenius at v, and $V_l(A)^\vee$ is the dual of $V_l(A)$.

It's a general fact (which follows from the Weil conjectures and the existence of the Néron model) that $L_v(A, T)$ is a polynomial with integer coefficients and is independent of the choice of l.

One defines the L-*function* of A/K to be

$$L(A/K,s)=\prod_v L_v(A,q_v^{-s})^{-1}.$$

Again, this can be shown to converge for $\mathrm{Re}(s)>3/2$ and conjecturally has meromorphic continuation to the whole of $\mathbb{C}$ satisfying a functional equation $s\leftrightarrow 2-s$.

4.2.2. *The Birch and Swinnerton–Dyer conjecture.* The Birch and Swinnerton–Dyer conjecture generalises naturally to all abelian varieties.

Conjecture 6. *Let K be a global field and A/K an abelian variety of dimension d. Let $0\neq\omega\in H^0(A,\Lambda^g\Omega^1_{A/K})$. Then*

(i) *We have the equality*

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

(ii) *The leading term of the Taylor series of $L(E/K,s)$ at $s=1$ is given by*

$$\frac{1}{r!}L^{(r)}(A/K,s)\mid_{s=1}=\frac{\mathrm{Reg}(A/K)}{|A(K)_{\mathrm{tors}}|\cdot|A^\vee(K)_{\mathrm{tors}}|}|Ш(A/K)|\prod_{v|\infty}\int_{A(K_v)}|\omega|_v\cdot\prod_{v\nmid\infty}c(A/K_v)\left|\frac{\omega}{\omega_v^o}\right|_v$$

$$\cdot\begin{cases}(\frac{2^{r_2}}{\sqrt{d_K}})^d & K\text{ number field}\\ (\frac{1}{q^{g-1}})^d & K\text{ function field}\end{cases}$$

(here r is the order of vanishing at $s=1$, r_2 is the number of complex places of K and ω_v^0 is the Néron differential*).*

The regulator and the non-archimedean factors deserve more explanation.

4.3. **The canonical height pairing on an abelian variety.** Recall that for each global field K and $n\geq 1$ we have a height function

$$h_{n,K}:\mathbb{P}^n(\bar{K})\to\mathbb{R}.$$

(Earlier we defined the height $h_{n,K}$ only on K points - for $P\in\mathbb{P}^n(K')$ for some finite extension K'/K, we define $h_{n,K}(P)=\frac{1}{[K':K]}h_{n,K'}(P)$.)

If $\mathcal{L}$ is a line bundle on A generated by (finitely many) global sections then we get an associated morphism $f_{\mathcal{L}}:A\to\mathbb{P}^n_K$ and we obtain a height function on $A(\bar{K})$ as

$$h_{\mathcal{L},K}=h_{n,K}\circ f_{\mathcal{L}}.$$

Strictly speaking we get a well defined map from $\mathcal{L}$ to

$$\frac{\{\text{functions } A(\bar{K})\to\mathbb{R}\}}{\{\text{bounded functions}\}}$$

due to the need to pick generating sections. We'll ignore this subtlety since, as in the elliptic curve case, the eventual height pairing will involve a limiting process that removes the ambiguity.

One can check that the association $\mathcal{L}\mapsto h_{K,\mathcal{L}}$ is additive in $\mathcal{L}$. This allows us to extend the definition of $h_{K,\mathcal{L}}$ to general line bundles: any line bundle $\mathcal{L}$ may be written as $\mathcal{L}_1\otimes$

$\mathcal{L}_2^{-1}$ for line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ generated by global sections (see [?MR0463157, Theorem 2.5.17]) and we set

$$h_{K,\mathcal{L}} = h_{\mathcal{L}_1,K} - h_{\mathcal{L}_2,K}.$$

So far we've constructed something like the naive height associated to a line bundle and we wish to pass to the canonical height. If $\mathcal{L}$ is symmetric ($[-1]^*\mathcal{L} \cong \mathcal{L}$) then $h_{K,\mathcal{L}}$ is a quadratic form up to a bounded function and we define

$$\hat{h}_{K,\mathcal{L}}(P) = \lim_{n\to\infty} \frac{1}{n^2} h(nP).$$

Similarly, if $\mathcal{L}$ is antisymmetric then $h_{K,\mathcal{L}}$ is additive up to a bounded function and we define

$$\hat{h}_{K,\mathcal{L}}(P) = \lim_{n\to\infty} \frac{1}{n} h(nP).$$

In general, we set

$$\hat{h}_{K,\mathcal{L}} = \frac{1}{2}\left(\hat{h}_{K,\mathcal{L}\otimes[-1]^*\mathcal{L}} + \hat{h}_{K,\mathcal{L}\otimes[-1]^*\mathcal{L}^{-1}}\right).$$

Now consider the abelian variety $A \times A^\vee$. This comes with the Poincare line bundle $\mathcal{P}$. We define the *canonical height pairing*

$$\langle\ ,\ \rangle : A(K) \times A^\vee(K) \to \mathbb{R}$$

by setting

$$\langle a, a' \rangle = \hat{h}_{K,\mathcal{P}}\left((a, a')\right).$$

This is bilinear, and non-degenerate modulo torsion on either side and we define the *regulator*

$$\mathrm{Reg}(A/K) = |\det((\langle P_i, P_j' \rangle)_{i,j}|$$

where $\{P_i\}$ is a basis for $A(K)/A(K)_{\mathrm{tors}}$ and $\{P_i'\}$ a basis for $A^\vee(K)/A^\vee(K)_{\mathrm{tors}}$.

Remark 4.3. An elliptic curve E is canonically isomorphic to its dual and the Poincare line bundle corresponds to the divisor $E \times (O) + (O) \times E$. One can use this to check that our definition recovers the previous height from the first lecture.

4.4. **The Néron model.** To explain the non–archimedean factors appearing in the statement of the Birch and Swinnerton–Dyer conjecture, we need to discuss the reduction theory of abelian varieties which takes the place of minimal Weierstrass equations in the elliptic curves case. It's a remarkable fact about abelian varieties that there exists a canonical 'best model', the Néron model.

Let F be a nonarchimedean local field, ring of integers $\mathcal{O}_F$, residue field k_F (one can define Néron models even over the ring of integers of a global field but we'll only be interested one prime at a time).

Theorem 4.4. *Let A/F be an abelian variety. Then there exists a smooth, separated, finite type group scheme $\mathcal{A}/\mathcal{O}_F$ with generic fibre A, satisfying the universal property (the* Néron mapping property*):*

for each smooth R-scheme $\mathcal{Y}/\mathcal{O}_F$, any F-morphism $\mathcal{Y}_F \to A$ extends uniquely to an $\mathcal{O}_F$-morphism $\mathcal{Y} \to \mathcal{A}$.

Example 4.5. Let E/F be an elliptic curve with good reduction. Then the minimal Weierstrass equation for E gives the Néron model of E.

Example 4.6. Let E/K be an elliptic curve over a function field $K = k(C)$ and let $\mathcal{E}/C$ be the associated elliptic surface. Then for each place v of K, the maximal smooth open subscheme of $\mathcal{E} \otimes_C \mathcal{O}_{K_v}$ is the Néron model of $E/\mathcal{O}_{K_v}$.

More generally, let E/F be an elliptic curve and $\mathcal{X}/\mathcal{O}_F$ be its minimal proper regular model. Then the Néron model $\mathcal{E}/\mathcal{O}_F$ is the maximal smooth open subscheme of $\mathcal{X}$.

Definition 4.7. The *reduction* of an abelian variety over F is the group variety $\tilde{A} = \mathcal{A} \times_{\mathcal{O}_F} k_F$ over k_F. If this is an abelian variety (i.e. if $\mathcal{A}$ is proper) then we say that A/F has *good reduction*.

The *identity component* of the Néron model, denoted $\mathcal{A}^0$ is the open subscheme whose special fibre is the connected component of the identity $\tilde{A}^0$ of $\tilde{A}$ (i.e. remove the closed subset consisting of the union of the (finitely many) components of the special fibre not containing the identity element).

Note that the Néron mapping property gives $A(F) = \mathcal{A}(\mathcal{O}_F)$ giving us a reduction homomorphism $A(F) \to \tilde{\mathcal{A}}(k_F)$. We write $A_0(F)$ for the points reducing to $\tilde{A}^0(k_F)$ and $A_1(F)$ for those points reducing to the identity.

The group $A(F)/A_0(F)$ is finite and we define the *Tamagawa number* $c(A/F)$ to be its order. If one defines $\Phi := \tilde{\mathcal{A}}/\tilde{\mathcal{A}}^0$ (an etale group scheme over k_F) then one has

$$c(A/F) = \Phi(\bar{k}_F)^{\mathrm{Gal}(\bar{k}_F/k_F)}.$$

(This is maybe a more conventional definition of the Tamagawa number, though less obviously a generalisation of the elliptic curve case.)

Remark 4.8. As with elliptic curves, it's a fact that an abelian variety over a global field has good reduction outside of a finite set of places. Moreover, one still has the Néron–Ogg–Shafarevich criterion: an abelian variety has good reduction at a place v if and only if the G_{K_v}-action on the l-adic Tate module for some l not equal to the characteristic of k_v is unramified.

Definition 4.9. Similarly to the case for A/F, one has that $\Lambda^d \Omega^1_{\mathcal{A}/\mathcal{O}_F}$ is a free $\mathcal{O}_{\mathcal{A}}$-module of rank 1. It is generated by a translation invariant form ω^o which is unique up to $\mathcal{O}_F^\times$. We refer to this as the *Néron differential*.

One can show, similarly to the case of elliptic curves, that

$$\int_{A(F)} |\omega^o| = \frac{c(A/K)|\tilde{A}^0(k_F)|}{q^d}$$

and, moreover, that

$$L(A/F, \frac{1}{q}) = \frac{|\tilde{A}^0(k_F)|}{q^d}.$$

This defines the remaining terms in the statement of the Birch and Swinnerton–Dyer conjecture. The discussion relating the terms of the conjecture to Adelic volumes goes through in this setting too.

4.5. **Accessing BSD data for Jacobians.** We now discuss the case where A is the Jacobian of a curve. Since equations for the Jacobian of even a simple curve can be extremely complicated, it is desirable from a computational (and also theoretical) point of view to be able to access invariants of the Jacobian 'on the level of the curve'. Here we give a few examples of how to do this.

4.5.1. *Tamagawa numbers.* Let F be a non-archimedean local field, C/F a curve and J/F its Jacobian. The following result is an arithmetic version of resolution of singularities for surfaces.

Theorem 4.10. *There exists a proper, regular, flat curve $\mathcal{C}$ over $\mathcal{O}_F$ with generic fibre isomorphic to C. Moreover, there is a unique 'smallest' such model, the minimal proper regular model, characterised by having no (-1)-curves in the special fibre.*

The main interest of this theorem for us is that a result of Raynaud [?MR1045822, Theorem 9.5.4] describes the Néron model of J in terms of the minimal regular model $\mathcal{C}$ of C (the precise description is quite involved, but, in particular, under quite general conditions (including when C is semistable, or when $C(F) \neq \emptyset$), the identity component of the Néron model agrees with $\mathrm{Pic}^0_{\mathcal{C}/\mathcal{O}_F}$ (the identity component of the relative Picard functor)). This gives us explicit control over $\tilde{J}^0/k_F$ in such cases.

This description of the Néron model yields the following theorem:

Theorem 4.11 ([?MR1717533, Theorem 1.1])**.** *Let C/K be a (smooth, proper, geometrically connected) curve, let $\mathcal{C}/\mathcal{O}_F$ be the minimal regular model of C, J/F the Jacobian of C and $\mathcal{J}/\mathcal{O}_F$ the Néron model of J. Denote by $\bar{C}$ the base-change to $\bar{k}_F$ of the special fibre of $\mathcal{C}$. Let $I = \{Z_1, ..., Z_n\}$ denote the irreducible components of $\bar{C}$ and let d_i denote their multiplicities. Define the map $\alpha : \mathbb{Z}^I \to \mathbb{Z}^I$ by*

$$Z_i \mapsto \sum_j (Z_i \cdot Z_j) Z_j$$

and extending linearly (here $Z_i \cdot Z_j$ is the intersection number of Z_i and Z_j) and let $\beta : \mathbb{Z}^I \to \mathbb{Z}$ be the map

$$Z_i \mapsto d_i$$

(and again extend linearly). Then $\mathrm{im}(\alpha) \subseteq \ker(\beta)$ and we have an isomorphism

$$\Phi_{\mathcal{J}}(\bar{k}_F) \cong \ker(\beta)/\mathrm{im}(\alpha),$$

equivariant for the action of $\mathrm{Gal}(\bar{k}_F/k_F)$.

Example 4.12. Consider the elliptic curve $E : y^2 = (x-1)(x-p)(x+p)$ over $\mathbb{Q}_p$ for p odd. This is a minimal Weierstrass equation for E whose reduction is a nodal cubic curve. The scheme

$$\mathcal{E}_0 = \mathrm{Proj}\left(\mathbb{Z}[x,y,z]/(y^2z - (x-z)(x-pz)(x+pz)\right)$$

is a projective, flat model of E, with a unique non-regular point at the node. Blowing up once here yields the minimal regular model, whose special fibre consists of two multiplicity one copies of $\mathbb{P}^1$, Z_1 and Z_2 say, intersecting transversally in two points.

Thus $\ker(\beta) = Z_1 - Z_2$ whilst $\mathrm{im}(\alpha) = 2(Z_1 - Z_2)$. In particular the Tamagawa number of $E/\mathbb{Q}_p$ is equal to 2 (note that we can already see this from the fact that, for an elliptic curve, the Néron model is the smooth part of the minimal regular model).

4.5.2. *Order of the Shafarevich–Tate group modulo squares.* For an elliptic curve E over a global field K, the *Cassels–Tate pairing* is an alternating, bilinear pairing

$$\langle\ ,\ \rangle_{\mathrm{CT}} : Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z}$$

which is non-degenerate on the quotient of $Ш(E/K)$ by its maximal divisible subgroup (which, of course, is conjecturally trivial).

In particular, if the order of $Ш(E/K)$ is finite, it is a square. Since computing $Ш(E/K)$ is notoriously difficult, when attempting to test the Birch and Swinnerton–Dyer conjecture computationally, one often computes all the other terms and then checks that the conjecture predicts that $|Ш(E/K)|$ is a square integer.

For a general abelian variety A/K, the generalisation of the Cassels–Tate pairing is a bilinear pairing

$$\langle\ ,\ \rangle_{\mathrm{CT}} : Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z}$$

which again has kernel the maximal divisible subgroup on each side.

When A/K is principally polarised (e.g. a Jacobian) the resulting pairing on $Ш(A/K)$ is *antisymmetric*. Thus its order, if finite, is either a square or twice a square. Poonen and Stoll famously showed that the latter can occur! (In fact, for a general abelian variety the order need not even be twice a square.)

We have the following result of Poonen and Stoll.

Theorem 4.13 ([?MR1740984, Theorem 8])**.** *Let K be a global field and A/K a principally polarised abelian variety with principal polarisation λ. Then there is an explicit class $c \in Ш(A/K)[2]$ such that, if finite, $Ш(A/K)$ has square order if and only if*

$$\langle c, \lambda(c)\rangle_{\mathrm{CT}} = 0.$$

Definition 4.14. Let F be a local field and C/F a curve of genus g (smooth, proper, geom. connected as usual). We say that C is *deficient* over F if it has no F-rational divisor of degree $g - 1$.

Theorem 4.15 ([?MR1740984, Corollary 12])**.** *In the notation of the previous theorem, if A is the Jacobian of a smooth projective curve C/K of genus g, then $c = \mathrm{Pic}^{g-1}_{C/K}$ and (as elements of $\mathbb{Q}/\mathbb{Z}$) we have*

$$\langle c, \lambda(c)\rangle_{\mathrm{CT}} = N/2$$

where (λ is the canonical principal polarisation on the Jacobian of C and) N is the number of deficient places *for C, i.e. the number of places v for which C is deficient over K_v.*

5. Exercises

Exercise 5.1. Consider the elliptic curve

$$E : y^2 = x^3 - x$$

over $\mathbb{Q}$, write $\omega = dx/2y$ and denote by Λ the period lattice of E (with respect to ω).

(i): Show that E has additive reduction at $p = 2$ and good reduction elsewhere. If you are familiar with Tate's algorithm, show that the reduction at 2 is type III and that $c(E/\mathbb{Q}_2) = 2$.

(ii): Compute the torsion subgroup of $E(\mathbb{Q})$ and, if you are familiar with two–descent computations, show that E has rank 0 over $\mathbb{Q}$.

(iii): Show[1] that we have

$$\int_{E(\mathbb{R})} |\omega| = 2\sqrt{\pi}\frac{\Gamma(1/4)}{\Gamma(3/4)}.$$

(iv): Show (via the identifcation $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ given in lectures) that the automorphism of E (defined over $\mathbb{Q}(i)$) given by

$$(x, y) \mapsto (-x, iy)$$

induces multiplication by i on $\mathbb{C}/\Lambda$ and deduce that we have

$$\Lambda = \sqrt{\pi}\frac{\Gamma(1/4)}{\Gamma(3/4)} \cdot \mathbb{Z}[i].$$

Exercise 5.2. Let K be a global function field with constant field q and E/K an elliptic curve. For each place v of K, let $\Delta_v \in K$ be the minimal discriminant of E at v (well defined up to units). Define the divisor

$$\mathcal{D}(E/K) := \sum_{v \in M_K} \mathrm{ord}_v(\Delta_v)(v).$$

We refer to this as the *minimal discriminant* of E/K.

Let ω be any non-zero regular differential on E/K. Show[2] that we have

$$\prod_{v \in M_K} \left|\frac{\omega}{\omega_v^o}\right|_v = q^{-\frac{1}{12}\deg \mathcal{D}(E/K)}.$$

Exercise 5.3. Let K be a global field and $E, E'/K$ two elliptic curves related by an isogeny $\phi : E \to E'$ of degree d (defined over K). Show that we have

$$\frac{\mathrm{Reg}(E/K)}{\mathrm{Reg}(E'/K)} = d^{\mathrm{rk}(E/K)}$$

[1] You may want to use the identity

$$2\int_0^{\pi/2} \cos^{2a-1}(\theta)\sin^{2b-1}(\theta)\ \mathrm{d}\theta = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

[2] [?MR2514094, Table 3.1] describing how various invariants of Weierstrass equations transform under a change of variable will be useful for this.

as elements of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

(You will need to use the fact that an isogeny and its dual are adjoints with respect to the canonical height pairing.)

Exercise 5.4. Consider the two elliptic curves

$$E : y^2 + y = x^3 + x^2 - 7x + 5 \qquad \Delta_E = -7 \cdot 13$$

and

$$E' : y^2 + y = x^3 + x^2 + 13x + 42 \qquad \Delta_{E'} = -7^3 \cdot 13^3.$$

They are related by a 3-isogeny $\phi : E \to E'$ given explicitly by the map

$$(x, y) \mapsto \left(\frac{x^3 - 2x^2 - 3x + 5}{(x-1)^2}, \frac{2x - 3 + (x^3 - 3x^2 + 7x - 7)y}{(x-1)^3} \right).$$

Define differentials $\omega = \frac{dx}{2y+1}$ and $\omega' = \frac{dx}{2y+1}$ on E and E' respectively.

In what follows we will prove the parity conjecture for $E/\mathbb{Q}$ under the assumption that $Ш(E/\mathbb{Q})$ is finite (via local computations rather than by computing the rank).

(i): Check that both equations are minimal at all primes and that both E and E' have split multiplicative reduction at 7 and 13, and good reduction elsewhere. Compute the Tamagawa numbers $c(E/\mathbb{Q}_7)$, $c(E/\mathbb{Q}_{13})$, $c(E'/\mathbb{Q}_7)$ and $c(E'/\mathbb{Q}_{13})$.

(ii): Show that we have

$$\phi^*(\omega') = \omega$$

and deduce that

$$\int_{E(\mathbb{R})} |\omega| = 3 \int_{E'(\mathbb{R})} |\omega'|.$$

From now on we assume that $Ш(E/\mathbb{Q})$ is finite.

(iii): Using parts (i) and (ii), show that we have

$$\frac{\mathrm{BSD}(E/\mathbb{Q})}{\mathrm{BSD}(E'/\mathbb{Q})} = 3a^2$$

for some rational number a.

(iv): Compute the root number $w(E/\mathbb{Q})$ and deduce that the parity conjecture holds for $E/\mathbb{Q}$.

Exercise 5.5. Let k be a finite field of order q, C/k a (smooth, projective, geometrically connected) curve and $K = k(C)$ its function field.

Let E_0/k be an elliptic curve and consider the constant elliptic curve $E = E_0 \times_k K$ over K. Write the Zeta function of E_0/k as

$$Z(E_0/k, T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}.$$

(i): Show, by considering the surface $\mathcal{E} = C \times E_0$ over k, that we have

$$\mathcal{L}(E, T) = Z(C, \alpha T) Z(C, \beta T).$$

(ii): Deduce that $L(E,s)$ has a meromorphic continuation to the whole complex plane with poles only on the lines $\mathrm{Re}(s) = 1/2$ and $\mathrm{Re}(s) = 3/2$. Show also that all its zeroes lie on the line $\mathrm{Re}(s) = 1$ and that it satisfies a functional equation $s \leftrightarrow 2 - s$.

(iii): If $C = \mathbb{P}^1$, show that the Birch and Swinnerton-Dyer conjecture predicts that E/K has rank 0. Prove this directly.

(iv): Still taking $C = \mathbb{P}^1$, show that the value of $L(E,s)$ at $s = 1$ is equal to

$$\frac{q}{|E(k)|^2}$$

and that

$$\mathrm{BSD}(E/K) = \frac{q|Ш(E/K)|}{|E(k)|^2}.$$

(v)*: Show that, in the same setting as (iv), the Shafarevich–Tate group of E/K is trivial.

Exercise 5.6. Have a look at the functions offered by MAGMA for computing with L-functions of elliptic curves over function fields[3]. Pick a few elliptic curves over, say, $\mathbb{F}_5(t)$. Compute their L-functions and anything else you wish to know about them and the associated elliptic surfaces using the MAGMA routines[4].

Exercise 5.7. Let $C : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$ with $f(x) \in \mathbb{Z}[x]$ monic, and let $J/\mathbb{Q}$ denote its Jacobian. Suppose that the discriminant of $f(x)$ is square free.

Show that the Tamagawa number $C(J/\mathbb{Q}_p)$ is equal to 1 for all odd primes p.

Exercise 5.8. Let p be an odd prime and $C/\mathbb{Q}_p$ be the hyperelliptic curve

$$C : y^2 = (x-2)((x-1)^2 - p^2)(x^2 - p^2).$$

Compute the Tamagawa number of its Jacobian.

Exercise 5.9. Let C be a hyperelliptic curve over $\mathbb{Q}_p$. Show that C is deficient if and only if it has even genus and no points over any odd degree extension.

[3]See https://magma.maths.usyd.edu.au/magma/handbook/text/1469.

[4]You can use the online MAGMA calculator http://magma.maths.usyd.edu.au/calc/ to do this.

Department of Mathematics, King's College London, Strand, London, WC2R 2LS.
Email address: adam.morgan@kcl.ac.uk