LECTURES ON THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

Benedict H. Gross

Carl Erickson and Jack Thorne prepared these notes from a preliminary version of my lectures, adding many examples and references. I want to thank them for their hard work, and to thank Mark Reeder for his comments.

CONTENTS

LECTURE 1: THE MORDELL-WEIL THEOREM

Torsion on elliptic curves. Let k be a field. An elliptic curve E is a curve of genus 1 over k, together with a distinguished k-rational

point $\mathcal{O}_E$. This curve can be defined as the locus in $\mathbb{P}^2$ of a non-singular cubic equation of the form:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where the coefficients a_i all lie in k; the curve is non-singular if and only if a certain polynomial $\Delta(a_1, \ldots, a_6)$ (the discriminant of the generalized Weierstrass equation) in the coefficients does not vanish. In this model, the distinguished point $\mathcal{O}_E = [0 : 1 : 0]$ is the unique point of the curve lying on the line $Z = 0$ at infinity. For this reason we often work with the inhomogeneous equation

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

If K/k is any field extension then the chord-tangent process turns $E(K)$, the set of points $P = (x, y)$ of E with coordinates in K, into an abelian group, with the zero element being $\mathcal{O}_E$. The addition law has the following property:

$$P + Q + R = 0 \Leftrightarrow P, Q, R \text{ are collinear.}$$

In particular, for a point $P = (x, y)$, the equality $P + (-P) + \mathcal{O}_E = \mathcal{O}_E$ tells us that

$$-P = (x, -y - a_1x - a_3).$$

In particular,

$$2P = \mathcal{O}_E \Leftrightarrow P = -P \Leftrightarrow 2y + a_1x + a_3 = 0. \tag{1}$$

A short calculation shows that this is equivalent to asking that x satisfy the cubic equation $4x^3 + b_2x^2 + 2b_4x + b_6 = 0$, where the b_i are certain polynomial functions in the a_i. The discriminant of this cubic equation is equal to $16 \cdot \Delta$. If k is of characteristic 2, this polynomial factors as $(a_1x + a_3)^2$; otherwise, as $\Delta \neq 0$ the roots of this polynomial are distinct and

$$E[2](K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

for any field K/k that contains these roots (If A is an abelian group, then $A[n]$ denotes the n-torsion of A).

Let k^s denote a separable closure of k. If $k^s \hookrightarrow \mathbb{C}$, then we have

$$E[n](k) \subset E[n](k^s) = E[n](\mathbb{C}) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Indeed, there is an analytic isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ of complex Lie groups, for some lattice $\Lambda \subset \mathbb{C}$. In particular, this implies the second isomorphism above.

To see the first equality, note that there exists a polynomial Q_n in two variables, with coefficients in k, with the property that $nP = \mathcal{O}_E$ if and only if $Q_n(x, y) = 0$. Therefore, if $\sigma \in \mathrm{Aut}(\mathbb{C}/k)$ and $nP = \mathcal{O}_E$, then P^σ is also an n-torsion point. In particular, P has only finitely

many conjugates over k; so its co-ordinates must in fact be algebraic over k.

In general, we have the following result.

Proposition 1. *Let n be a positive integer prime to the characteristic of k.*

$$E[n](k^s) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

On the other hand, if k is of characteristic 2 then we have seen that $E[2](k)$ is either a cyclic group of order 2 (if $a_1 \neq 0$), or is trivial (if $a_1 = 0$). Indeed, the non-trivial 2-torsion points correspond to roots of the polynomial $a_1 x + a_3 = 0$.

A standard reference for the results described above, which does not assume a large amount of algebraic geometry, is [47]. For proofs using scheme-theoretic language, in the more general setting of abelian varieties, see [39].

Galois cohomology. We continue with E/k as before. Let $n > 1$ be an integer prime to the characteristic, and fix a choice of separable closure k^s. There is an exact sequence of Galois modules

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow[\times n]{} E \longrightarrow 0.$$

When we write E or $E[n]$ here, we really mean the points over k^s. Taking the long exact sequence in Galois cohomology, we get

$$E(k) \xrightarrow[\times n]{} E(k) \longrightarrow H^1(k, E[n]) \longrightarrow H^1(k, E) \xrightarrow[\times n]{} H^1(k, E).$$

This gives us a short exact sequence

$$0 \longrightarrow E(k)/nE(k) \xrightarrow[\delta]{} H^1(k, E[n]) \longrightarrow H^1(k, E)[n] \longrightarrow 0.$$

The map δ sends the equivalence class of P to the cohomology class of the cocycle $\sigma \mapsto Q^\sigma - Q$, where Q is any point in $E(k^s)$ with the property that $nQ = P$.

We now specialize to the case that $n = 2$, and suppose that the characteristic of k is $\neq 2$ and that all of the points of $E[2]$ are already defined over k. Then our curve E can be given by an equation of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

which has $\Delta = 16 \prod (e_i - e_j)^2$. If B denotes the group $k^\times/(k^\times)^2$, written multiplicatively, we have an isomorphism (described below)

$$H^1(k, E[2]) \cong \{(b_1, b_2, b_3) \in B^3 : b_1 \cdot b_2 \cdot b_3 = 1\} = B_1^3.$$

Lemma 2. *With this identification, the map δ is given by the formula $\delta(P) = (x - e_1, x - e_2, x - e_3)$ in B_1^3 (suitably interpreted - if one of these entries vanishes, then we replace it with any element making the triple lie in the above subgroup).*

Proof. The proof is based on the existence of the Weil pairing (cf. Ch. III of [47]) $e_2 : E[2] \times E[2] \to \mu_2$. It is bilinear, strictly alternating, and non-degenerate, so gives an injective homomorphism $E[2] \to \mu_2^3$ defined by

$$P \mapsto (e_2(P, T_1), e_2(P, T_2), e_2(P, T_3))$$

where $T_i = (e_i, 0)$ are the three non-trivial 2-torsion points. The image consists of the subgroup with product equal to 1, and Kummer theory provides the isomorphism used above.

We define the Weil pairing e_2 as follows. Given a 2-torsion point T_i, find functions f_i, g_i in the function field $k(E)$ of E with the property that $\operatorname{div} f_i = 2T_i - 2\mathcal{O}_E$, and $f_i \circ [2] = g_i^2$. In our case, we can take $f_i = x - e_i$, and define $e_2(S, T_i) = g_i(S + X)/g_i(X)$ for any point X such that $g_i(S + X)$ and $g_i(X)$ are both defined and not zero.

Now take $P \in E(k)$, and let $Q \in E(k^s)$ be such that $2Q = P$. Then with the given identifications we have

$$\delta : P \mapsto Q^\sigma - Q = (e_2(Q^\sigma - Q, T_i))_i = (g_i(Q^\sigma - Q + X)/g_i(X))_i.$$

If $P \neq T_i$ then on taking $X = Q$ we have

$$g_i(Q^\sigma - Q + X)/g_i(X) = g_i(Q^\sigma)/g_i(Q)$$

$$= g_i(Q)^\sigma / g_i(Q) = \sqrt{f_i(P)}^\sigma / \sqrt{f_i(P)}.$$

The result follows. □

Let us now suppose that k is a global field, that is, a number field or the function field of a non-singular projective curve defined over a finite field. Let S be the set of places v which are either archimedean, or divide 2, or such that the e_i are not all integral at v, or such that $v(\Delta) \neq 0$. Note that S is a finite set. (We will see later that the curve E has good reduction at all places v which are not in the finite set S.)

Lemma 3. *For any $v \notin S$, and for any point $P = (x, y)$ in $E(k_v)$, $v(x - e_i)$ is even for all i.*

Proof. Suppose first that $v(x - e_i) < 0$ for some, and hence all, i. Then $v(x - e_i)$ does not depend on i and the defining equation of E shows that $3v(x - e_i) = 2v(y)$, giving the result.

Suppose instead that $v(x-e_i)>0$ for some i. Since $v(\Delta)=0$, we have $v(e_i-e_j)=v(x-e_j-x+e_i)=0$ for $j\neq i$, so $v(x-e_j)=0$. Hence $v(x-e_i)=2v(y)$. □

The above lemma shows that $E(k)/2E(k)$ injects into the subgroup of B_1^3 consisting of those elements with $v(\alpha_i)$ even whenever v is not in S. But this subgroup is finite: let $k^\times(S,2)/(k^\times)^2\subset k^\times/(k^\times)^2$ be the subgroup of elements with even valuation outside of S, and let A_S be the ring of S-integers of k; that is, the subring of k consisting of elements having non-negative valuation at all places outside S. Then there is an exact sequence

$$1\longrightarrow A_S^\times/(A_S^\times)^2\longrightarrow k^\times(S,2)/(k^\times)^2\longrightarrow \mathrm{Pic}(A_S)[2]\longrightarrow 1$$

and the outside two terms are both finite, by the finiteness of the class group $\mathrm{Pic}(A_S)$ and the finite generation of the unit group $A_S^\times$ of A_S. It follows that $E(k)/2E(k)$ is finite.

For general n one defines two groups as follows. For every place v we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(k)/nE(k) & \xrightarrow{\delta} & H^1(k,E[n]) & \longrightarrow & H^1(k,E)[n] & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(k_v)/nE(k_v) & \xrightarrow{\delta} & H^1(k_v,E[n]) & \longrightarrow & H^1(k_v,E)[n] & \longrightarrow & 0
\end{array}$$

Definition 4. The *n-Selmer group* is the group of those elements of $H^1(k,E[n])$ whose restriction to $H^1(k_v,E[n])$ lies in the image of the group $E(k_v)/nE(k_v)$ for all places v. In other words, we take

$$\mathrm{Sel}_n(k,E)=\ker\left(H^1(k,E[n])\to\prod_v H^1(k_v,E)\right).$$

The *Tate-Shafarevitch group* is defined by

$$Ш(k,E)=\ker\left(H^1(k,E)\to\prod_v H^1(k_v,E)\right).$$

We then have an exact sequence

$$0\longrightarrow E(k)/nE(k)\longrightarrow \mathrm{Sel}_n(k,E)\longrightarrow Ш(k,E)[n]\longrightarrow 0.$$

One can show, using the classical finiteness theorems of algebraic number theory, that the n-Selmer group is always finite. This proves that the two groups $E(k)/nE(k)$ and $Ш(k,E)[n]$ are both finite, for any integer $n\geq 1$. The first finiteness statement is called the *weak Mordell-Weil theorem.*

A proof of this theorem in the general case can be found in Ch. VIII of [47], or Ch. 4 of [37].

Reduction modulo v. One element of the proof of the finiteness of the n-Selmer group is the notion of the reduction of elliptic curves modulo a prime, to which we now turn. Let k_v be a field complete with respect to a normalized discrete valuation v. For us these will arise as the completions at finite places of global fields. From now on we write A_v for the ring of integers, π_v for a choice of uniformizer of this discrete valuation ring, and $\mathbb{F}_v$ for the residue field $A_v/\pi_v A_v$.

Take an elliptic curve E/k_v. Let us choose an equation for E such that the a_i are all in A_v, and such that $v(\Delta(a_1,\ldots,a_6))$ is minimal with respect to this property. This is called a *minimal equation* for E. Write $\bar{a}_i$ for the image of a_i in $\mathbb{F}_v$. One can show that the reduced curve

$$y^2 + \bar{a}_1 xy + \bar{a}_3 y = x^3 + \bar{a}_2 x^2 + \bar{a}_4 x + \bar{a}_6$$

does not depend on the choice of minimal equation (at least, up to isomorphism over the residue field). It therefore has the right to be called the reduction of E modulo v, and we will write it as $\widetilde{E}_v$, or $\widetilde{E}$ if no confusion will result.

Definition 5. If $v(\Delta) = 0$, then $\widetilde{E}$ will be non-singular, and so will be an elliptic curve. In this case, we say that E has *good reduction at* v. If $v(\Delta) > 0$ then the reduced curve will be singular, in which case we say that E has *bad reduction.* However, the non-singular locus $\widetilde{E}^{ns}$ can still be made into a group variety using the same chord-tangent process, with the point at infinity still playing the role of zero element. There are three possibilities.

(1) $\widetilde{E}$ is a cuspidal cubic curve. In this case, $\widetilde{E}^{ns}$ is isomorphic to the additive group $\mathbb{G}_a$.
(2) $\widetilde{E}$ is a nodal cubic curve, and the tangent lines at the node are defined over the residue field. In this case, $\widetilde{E}^{ns}$ is isomorphic to the multiplicative group $\mathbb{G}_m$.
(3) $\widetilde{E}$ is a nodal cubic curve, and the tangent lines at the node are defined only over a quadratic extension of the residue field. In this case, $\widetilde{E}^{ns}$ is isomorphic to the twisted form of the multiplicative group corresponding to this quadratic extension.

We speak respectively of *additive, split multiplicative, and non-split multiplicative reduction.*

Example. Consider the curve

$$E : y^2 = x(x-1)(x-t)$$

over the function field $k = \mathbb{F}_q(t)$ of genus 0, where q is odd. This curve has discriminant $\Delta = 16 \cdot t^2 \cdot (t-1)^2$. Since a change of variable changes the valuation of Δ at each place by a multiple of 12, the above equation is minimal at all places except $t = \infty$. At the place $t = 1$, the curve E has split multiplicative reduction. At the place $t = 0$ the curve E has multiplicative reduction, and the tangents at the node are rational if and only if -1 is a square in $\mathbb{F}_q$. We will see that the curve E has additive reduction at $t = \infty$.

One of the reasons that the notion of reduction is useful is the existence of a natural reduction map $\rho : E(k_v) \to \widetilde{E}(\mathbb{F}_v)$. Choose a minimal equation for E over A_v. Given a point $P = [X : Y : Z]$ with co-ordinates in k_v, one can assume that each co-ordinate is integral, and that at least one of X, Y, Z has valuation 0. The point $\rho(P) = [\bar{X}, \bar{Y}, \bar{Z}]$ then lies on the reduced curve. There are some important subgroups associated to the map ρ.

Definition 6. We write

$$E^0(k_v) = \rho^{-1}(\widetilde{E}^{ns}(\mathbb{F}_v))$$

for the inverse image of the smooth locus on the reduced curve (if E has good reduction, then $E(k_v) = E^0(k_v)$). We write

$$E^1(k_v) = \rho^{-1}(\mathcal{O}_{\widetilde{E}})$$

for the inverse image of the point at infinity on the reduced curve.

Proposition 7. *The restriction of ρ to $E^0(k_v)$ is a homomorphism, and surjects onto $\widetilde{E}^{ns}(\mathbb{F}_v)$.*

Moreover, if n is prime to the residue characteristic and E has good reduction at v, then the restriction of ρ to the n-torsion of $E(k_v)$ is also injective, and so induces an isomorphism

$$E(k_v)[n] \cong \widetilde{E}^{ns}(\mathbb{F}_v)[n].$$

Proof. The surjectivity follows from a version of Hensel's lemma. The fact that ρ is a homomorphism follows on showing that the chord-tangent process behaves well with respect to reduction.

There is a complete description of the kernel of the reduction map in terms of the formal group attached to E, giving the addition law in a neighborhood of the identity. It is known that all the torsion in the kernel has order a power of the residue characteristic; this gives the second part of the proposition. For the definition of the associated formal group, see Ch. IV of [47] or Thm. 4.2 in [49] . An introduction to one-dimensional formal groups in general can be found in [19]. □

Descent computations. One of the reasons for introducing the Selmer group is that it is effectively computable. In this section we will briefly describe the procedure in a special case and then carry it out for two curves which will be of interest in later lectures.

We will again consider the case where E is an elliptic curve over a global field k, not of characteristic 2, and all the points of $E[2]$ have co-ordinates in k. In this case, E can be written in the form

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

and we continue to write $T_i = (e_i, 0)$.

Let S denote the set of places of k which divide 2 or where E has bad reduction, together with the infinite places. Lemma 3 shows that we have injections

$$E(k)/2E(k) \hookrightarrow \mathrm{Sel}_2(k, E) \hookrightarrow (k^\times(S, 2)/(k^\times)^2)_1^3$$

the latter group being finite. In order to compute the Selmer group exactly we must compute the local conditions at v imposed by the image of $E(k_v)/2E(k_v)$ in $H^1(k_v, E[2])$, for every place v.

In fact, the group on the right above is the one obtained by imposing the local conditions at places not in S. In other words,

$$(k^\times(S, 2)/(k^\times)^2)_1^3 = \ker\left(H^1(k, E[2]) \to \prod_{v \notin S} H^1(k, E)\right).$$

It remains therefore to compute the conditions at the finitely many places $v \in S$. This can be done using the explicit description of the map δ given earlier.

Proposition 8. *A triple*

$$(b_1, b_2, b_3) \in (k^\times(S, 2)/(k^\times)^2)_1^3$$

not lying in $\delta(E[2])$ *lies in* $\mathrm{Sel}_2(k, E)$ *if and only if for every* $v \in S$ *there exists a solution* (z_1, z_2, z_3) *in* k_v *with* $z_1 z_2 z_3 \neq 0$ *to the following pair of equations:*

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$$
$$b_1 z_1^2 - b_3 z_3^2 = e_3 - e_1.$$

Proof. Suppose that (b_1, b_2, b_3) does lie in the 2-Selmer group. Without loss of generality, we may suppose that $b_1 b_2 = b_3$. We must be able to produce, for every $v \in S$, a solution to the equations

$$b_1 z_1^2 = x - e_1$$
$$b_2 z_2^2 = x - e_2$$
$$b_3 z_3^2 = x - e_3$$
$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

with values in k_v. Then one has

$$b_1 z_1^2 = e_2 - e_1 + b_2 z_2^3 = e_3 - e_1 + b_3 z_3^2,$$

proving necessity. On the other hand, given a solution to the equations in the statement of the proposition, one can take

$$x = b_1 z_1^2 + e_1 \text{ and } y = b_1 b_2 z_1 z_2 z_3,$$

and then (x, y) is a point in $E(k_v)$ mapping to our given triple. □

The computation of the Selmer group is therefore reduced to the problem of deciding whether finitely many curves have points defined over local fields. This is a simple matter, using Hensel's lemma. With this information in hand, we will compute an example.

Example. Take $k = \mathbb{F}_q(t)$ with q odd, and let E be the elliptic curve

$$E : y^2 = x(x-1)(x-t).$$

The computation of the Selmer group at 2 splits into two cases, depending on whether or not -1 is a square in $\mathbb{F}_q^\times$, although we will see that the final answer is the same:

$$\mathrm{Sel}_2(k, E) = (\mathbb{Z}/2\mathbb{Z})^2.$$

Suppose first that -1 is a square, and let α be a non-square in $\mathbb{F}_q^\times$. The above curve has bad reduction at the places $t = 0, 1$ and ∞, and good reduction elsewhere. We can therefore take $S = \{0, 1, \infty\}$, and the pair (b_1, b_2) can take the values $(\alpha^a t^b (t-1)^c, \alpha^d t^e (t-1)^f)$, where $a, \ldots, f$ are allowed to take the values 0 or 1.

Before beginning the descent computation we note a shortcut which is often useful. At each place v of k, we have the filtration

$$E(k_v) \supset E^0(k_v) \supset E^1(k_v).$$

Write $C = E(k_v)/E^1(k_v)$. Since $E^1(k_v)$ can be represented as the set of points of a formal group in $\pi_v A_v$, where multiplication by 2 is an isomorphism ([47], Prop. IV.2.3(b)), $E(k_v)/2E(k_v)$ is isomorphic to $C/2C$.

Now, C has a natural filtration whose quotients are $E(k_v)/E^0(k_v)$ and $E^0(k_v)/E^1(k_v) \cong \widetilde{E}_v^{ns}(\mathbb{F}_v)$. The latter group is easily understood, and the first group can be computed using Tate's algorithm to compute the Néron model of an elliptic curve, cf. [49] or [48], chapter IV. Once enough is known about the group $C/2C$, it can sometimes be shown that the elements of $E[2]$ give a complete set of representatives, immediately giving the local conditions at v.

In the language of the above references, the curve E has multiplicative reduction of Kodaira type I_2 at the places 0 and 1, and additive

reduction of Kodaira type I_2^* at infinity. Looking at the table on page 46 of [49] (also Table 15.1 in [47]) shows that when $u = \infty$,

$$E(k_u)/E^0(k_u) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The group $\widetilde{E}_u^{ns}(\mathbb{F}_u)$ has no 2-torsion, so in this case we see that

$$E(k_u)/2E(k_u)$$

is an abelian group of the same type.

Now, computing the map δ on the 2-torsion of E locally at the place u gives

$$\begin{array}{rcl} \mathcal{O}_E & \mapsto & (1,1) \\ (0,0) & & (t,-1) \equiv (t,1) \\ (1,0) & & (1,1-t) \equiv (1,t) \\ (t,0) & & (t,t-1) \equiv (t,t), \end{array}$$

so we are in the case described above. Applying these local conditions implies that a set of representatives for the 2-Selmer group is contained in the set of elements $(t^b(t-1)^c, t^e(t-1)^f)$. At this point it is instructive to draw a table:

b_2 \ b_1	1	t	$t-1$	$t(t-1)$
1	$\mathcal{O}_E$	$(0,0)$		
t				
$t-1$	$(1,0)$	$(t,0)$		
$t(t-1)$				

The entries above indicate that a point in $E(k)$ maps to the given pair (b_1, b_2), which must therefore lie in the 2-Selmer group. To decide whether the remaining entries lie in the Selmer group, we argue using the proposition above. Note that the conditions at ∞ have already been imposed, so we need only check for points on the corresponding curves in the completions at 0 and 1.

Consider the pair $(b_1, b_2) = (t-1, 1)$. This corresponds to the pair of equations

$$(t-1)z_1^2 - z_2^2 = 1$$

and

$$(t-1)z_1^2 - (t-1)z_3^2 = t.$$

Let w be the normalized discrete valuation at $t-1$. If (z_1, z_2, z_3) is a solution in k_w with $z_1 z_2 \neq 0$, then the first equation shows that $w(z_1) \geq 0$. Then the second equation gives $1 + 2w(z_3) = 0$, a contradiction. It follows that the system of equations has no solution in k_w, and hence $(t-1, 1)$ is not in the 2-Selmer group.

Using the fact that if $x \in \mathrm{Sel}_2(k,E)$ but $y \notin \mathrm{Sel}_2(k,E)$ then $xy \notin \mathrm{Sel}_2(k,E)$, we arrive at the following table.

b_2 \ b_1	1	t	$t-1$	$t(t-1)$
1	$\mathcal{O}_E$	$(0,0)$	X	X
t				
$t-1$	$(1,0)$	$(t,0)$	X	X
$t(t-1)$				

A cross indicates an element that does not lie in the 2-Selmer group. One can now check that neither of the pairs $(1,t)$ or $(t-1,t)$ lie in the 2-Selmer group, giving the following table.

b_2 \ b_1	1	t	$t-1$	$t(t-1)$
1	$\mathcal{O}_E$	$(0,0)$	X	X
t	X	X	X	X
$t-1$	$(1,0)$	$(t,0)$	X	X
$t(t-1)$	X	X	X	X

It follows that

$$\mathrm{Sel}_2(k,E) = E(k)/2E(k) \cong E[2] = (\mathbb{Z}/2\mathbb{Z})^2.$$

In particular, the curve E has no rational points except for 2-torsion (it is a simple matter to check that E has no torsion except for 2-torsion). In the case that -1 is not a square in $\mathbb{F}_q^\times$ one can proceed similarly, aided by the fact that $E[2]$ now generates $E(k_w)/2E(k_w)$ at the place w used above. Hence $E(k) \cong (\mathbb{Z}/2\mathbb{Z})^2$ and $Ш(k,E)[2] = 0$.

Example. Let

$$E' : t(t-1)y^2 = x(x-1)(x-t).$$

This is a twist of E, in the sense that it becomes isomorphic to E over the separable quadratic extension obtained by adjoining $\sqrt{t(t-1)}$, via the substitution $\sqrt{t(t-1)}y \mapsto y$. This curve E' now has additive reduction of type I_2^* at the three places $t = 0, 1$ and ∞, and good reduction elsewhere. One can check that the natural map $E'[2] \to E'(k_v)/2E'(k_v)$ is an isomorphism at these 3 places, allowing one to immediately calculate the 2-Selmer group. One obtains

$$\mathrm{Sel}_2(k,E') \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } -1 \text{ is not a square in } \mathbb{F}_q^\times; \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{if } -1 \text{ is a square in } \mathbb{F}_q^\times. \end{cases}$$

In the next lecture, we will compare these results with those predicted by the conjecture of Birch and Swinnerton-Dyer.

Heights. Let k be a global field, and E/k an elliptic curve. Let n be a non-zero integer. The finiteness of $E(k)/nE(k)$ is a necessary condition for the finite generation of $E(k)$, but by no means a sufficient one. For example, $E(\mathbb{C})/nE(\mathbb{C})$ is trivial for all $n \neq 0$. To extract a proof of the full Mordell-Weil theorem from the weak version, we introduce the Néron-Tate height. This is a pairing $\langle , \rangle : E(k) \times E(k) \to \mathbb{R}$ such that:

(1) $\langle , \rangle$ is biadditive and symmetric.
(2) For all $P \in E(k)$, $\langle P, P \rangle \geq 0$.
(3) For all $M > 0$, the set of points P such that $\langle P, P \rangle \leq M$ is finite.

Remark. The existence of such a pairing has the immediate corollary that the torsion group $E(k)_{\text{tors}}$ is finite. In fact, one can show that a point P is torsion if and only if $\langle P, P \rangle = 0$.

We will give the definition of the height pairing on the Jacobian of a curve in lecture 3. In the case that $k = \mathbb{Q}$, an approximation to the height can be given as follows. Taking a point to its x co-ordinate gives a map from E to $\mathbb{P}^1$, defined over $\mathbb{Q}$. Writing $x(P) = a/b$ with a, b coprime integers, we define the logarithmic height to be $h(P) = \log \max(|a|, |b|)$. Then the difference $\langle P, P \rangle - h(P)$ is bounded as P ranges over $E(\mathbb{Q})$.

With this in hand, we can deduce the full Mordell-Weil theorem.

Theorem 9. *Let k be a global field, E/k an elliptic curve. Then $E(k)$ is a finitely generated abelian group.*

Proof. Choose an integer $n > 1$, and let the points $P_1, \ldots, P_r$ be representatives for the finite group $E(k)/nE(k)$. Let $M = \max_i(\langle P_i, P_i \rangle)$, and let T be the set of points P such that $\langle P, P \rangle \leq M$. This is a finite set.

In fact, the points in T generate $E(k)$. Otherwise, there exists a point Q of minimal height which is not in the span of T. Since the P_i represent the cosets of $nE(k)$, there exists an i and a point R in $E(k)$ such that $Q - P_i = nR$. Since Q and P_i are not collinear in the Euclidean space $E(k) \otimes \mathbb{R}$, we find

$$\langle Q - P_i, Q - P_i \rangle < 4 \cdot \langle Q, Q \rangle,$$

so

$$n^2 \cdot \langle R, R \rangle < 4 \cdot \langle Q, Q \rangle.$$

By the minimality of the height of Q, the point R must lie in the span of T. This implies that the same is true of $Q = nR + P_i$, which is the desired contradiction. □

With this theorem in hand we can define an important invariant of elliptic curves over global fields.

Definition 10. Let $P_1, \ldots, P_n$ be a basis for a free subgroup of $E(k)$ of finite index I. The *regulator of* E is defined to be the positive real number

$$R(E/k) = \det(\langle P_i, P_j \rangle)/I^2.$$

One can check that this definition does not depend on the choice of P_i. For example, if $E(k)$ is finite, then $R(E/k) = 1/\#E(k)^2$.

We will see in lecture 3 that when E is an elliptic curve over a global function field $k = \mathbb{F}_q(X)$, then $\langle P, Q \rangle$ is a rational multiple of $\log q$, where the denominator is controlled by the places of bad reduction. The regulator $R(E/k)$ is then a positive rational multiple of $(\log q)^n$.

The theory of heights is developed for elliptic curves in [47]. A rather direct approach, treating just the case when $k = \mathbb{Q}$, can be found in [9]. For a discussion of Néron's theory of local heights on curves, see [22], or the discussion in the third lecture.

Lecture 2: Conjectures on L-functions

Before discussing the conjecture of Birch and Swinnerton-Dyer, we must define the L-function of an elliptic curve over a global field k. It is given as an Euler product, the factors being indexed by the finite places of k. We begin by defining the incomplete L-function, which omits the finite number of places at which E has bad reduction.

The incomplete L-function. Let E be an elliptic curve defined over k. Let S be the finite set of places of k consisting of the infinite places and the places where E has bad reduction. As discussed above, for all places $v \notin S$, there is a model of E with the coefficients a_i lying in the local ring A_v at v and the discriminant $\Delta = \Delta_v$ is a unit in A_v. In this case, we get an elliptic curve $\widetilde{E}_v$ over the residue field $\mathbb{F}_v = A_v/\pi_v A_v$, a finite field of cardinality q_v.

The following theorem is fundamental for elliptic curves over finite fields.

Theorem 11 (Hasse). *Write* $\#\widetilde{E}_v(\mathbb{F}_v) = 1 + q_v - a_v$, *where* $v \notin S$. *Then*

$$a_v^2 \leq 4q_v,$$

so the roots of the polynomial

$$h_v(t) = 1 - a_v t + q_v t^2 = (1 - \alpha_v X)(1 - \bar{\alpha}_v X)$$

lie in an imaginary quadratic field. Furthermore, if $F_n/\mathbb{F}_v$ is the unique field extension of degree $n \geq 1$, then

$$\#\widetilde{E}_v(F_n) = (q_v^n + 1) - (\alpha_v^n + \bar{\alpha}_v^n).$$

Proof. See [47], Thm. V.1.1. □

These point counts on E over finite places are the key ingredient in defining its corresponding L-function. The polynomial $h_v(t)$ is the reciprocal of the *formal local L-factor* of an elliptic curve over a finite field:

$$L(\widetilde{E}_v/\mathbb{F}_v, t) = h_v(t)^{-1}.$$

Substitute q_v^{-s} for t to get the local L-factor

$$L_v(E/k, s) = L(\widetilde{E}_v/\mathbb{F}_v, q^{-s}) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}. \tag{2}$$

Definition 12. With notation as above, the *incomplete L-function* of E is

$$L_S(E/k, s) = \prod_{v \notin S} L_v(E/k, s). \tag{3}$$

Both this infinite product, and the Dirichlet series $L_S(E/k, s) = \sum_{n \geq 1} a_n n^{-s}$ with integral coefficients which is formally assembled from it converge absolutely in the half plane $\mathrm{Re}(s) > 3/2$. This follows from the estimate in the above theorem and comparison with the Dedekind zeta-function of k. Note that when k is a function field, this Dirichlet series is of the form $\sum_{m \geq 0} b_m q^{-ms}$ where q is the cardinality of the constant field of k.

The formal Euler product (3) determines E up to isogeny over k. Before defining the complete L-function, we describe how this works.

Interlude on the isogeny theorem.

Definition 13. Let l be a prime and let E/k be an elliptic curve. The *l-adic Tate module* of E is

$$T_l E = \varprojlim_n E[l^n],$$

the limit being taken over the natural numbers with respect to the homomorphisms

$$E[l^{n+1}] \xrightarrow[\times l]{} E[l^n].$$

Observe that $T_l E$ has a natural profinite topology, and a continuous action of $\mathrm{Gal}(k^s/k)$. When l is prime to the characteristic, Proposition 1 implies that $T_l E$ is a free $\mathbb{Z}_l$-module of rank 2. We will often use the 2-dimensional vector space $V_l E = T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, over $\mathbb{Q}_l$. This has

$L_v(E,s) = \det(1 - \sigma_v q_v^{-s} \mid T_\ell(E))^{-1}$

vs $= \det(1 - \sigma_v^{-1} q_v^{-s} \mid T_\ell(E)^\vee)^{-1}$ ← right way to define

↑ geo Frob

Note since $T_\ell(E)$ is semisimple, get same e.vs. when looking at σ_v^{-1} on the dual.

a continuous action of $\mathrm{Gal}(k^s/k)$, and gives (after a choice of basis) a 2-dimensional l-adic Galois representation

$$\rho_{E,l} : \mathrm{Gal}(k^s/k) \to \mathrm{GL}_2(\mathbb{Q}_l).$$

When k is a global field, one can show that this representation is unramified away from the finite collection of places $S(l)$ of k, which divide l or where the curve E has bad reduction. For each finite place $v \notin S(l)$ let ϕ_v denote a choice of arithmetic Frobenius element in $G_{S(l)}$, the Galois group of the maximal extension of k which is unramified outside of $S(l)$. Then $\rho_{E,l}(\phi_v)$ has characteristic polynomial

$$X^2 - a_v X + q_v \text{ for } v \notin S. \tag{4}$$

The element ϕ_v is defined only up to conjugacy in $G_{S(l)}$ but the characteristic polynomial is independent of this choice. Since $S(l)$ is finite, the Chebotarev density theorem implies that the set $\{\phi_v\}_{v \notin S}$ is dense in $G_{S(l)}$. By continuity, the terms in the Euler product defining the incomplete L-function determine the characteristic polynomials of $\rho_{E,l}(\sigma)$ for all $\sigma \in G_{S(l)}$. In particular, knowledge of the Euler product of $L_S(E/k, s)$ determines the representation $\rho_{E,l}$ up to isomorphism, provided that this representation is semi-simple, which was proved by Serre cf. [43], I-10.

Tate conjectured that the natural map

$$\mathrm{Hom}_k(E, E') \otimes \mathbb{Z}_l \to \mathrm{Hom}_{\mathrm{Gal}(k^s/k)}(T_l E, T_l E'), \tag{5}$$

known to be injective ([47],Thm. 7.4), is in fact an isomorphism, whenever k is a field finitely generated over the prime field. He proved this for abelian varieties in the case when k is a finite field [50], and Serre proved it for elliptic curves when k is a number field, under the assumption that E has a place of multiplicative reduction [43]. Finally, Faltings proved the full conjecture for all abelian varieties [18], [14]. In particular, two elliptic curves are isogenous if and only if the associated l-adic representations are isomorphic.

Thus the Euler product defining the incomplete L-function is a complete isogeny invariant of elliptic curves over global fields. More notes on this section may be found in [47], Ch. 3, §7.

The L-function of an elliptic curve. The general formalism of L-functions suggests that the L-function of an elliptic curve E over a global field k should have a meromorphic continuation to the whole of $\mathbb{C}$ and satisfy a functional equation. Before this can be true we must add some factors to the incomplete L-function, corresponding to the infinite places and the finite places of bad reduction.

Recall that S is the set of infinite places, together with the places where E has bad reduction. For finite $v \in S$, we define the local L-factor

$$L_v(s) = \begin{cases} 1 & \text{if } E \text{ has additive reduction at } v; \\ (1-q_v^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } v; \\ (1+q_v^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } v. \end{cases} \tag{6}$$

A commonality between L-factors at good and bad finite places is that

$$L_v(1) = \frac{q_v}{\#\widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v)}, \tag{7}$$

where $\widetilde{E}_v^{\mathrm{ns}}$ is the smooth locus of the reduction of a minimal model for E over A_v.

The following two quantities measure bad reduction.

Definition 14. The *minimal discriminant* of an elliptic curve E over a number field (resp. global function field) k is the integral ideal of k (resp. positive divisor of the curve associated to the function field k) defined by

$$\mathcal{D}(E/k) = \prod_{v \nmid \infty} \mathfrak{p}_v^{v(\Delta_v)},$$

where Δ_v is the discriminant of a minimal equation for E/k_v and $\mathfrak{p}_v$ is the prime ideal (resp. prime divisor) associated to the finite place v.

Remark. Suppose that k is a number field, with ring of integers A. We say that a Weierstrass model for E is a *global minimal model* if it is a minimal model at all finite places v of k. Such a model exists if and only if a certain projective A-module of rank 1, corresponding to the Néron differentials, has trivial class in $\mathrm{Pic}(A)$. If such a model exists, then the discriminant ideal $\mathcal{D}(E/k)$ is principal, generated by the discriminant Δ of a global minimal model. For more details, see [47], Ch. VIII, §8.

Definition 15. The *conductor* of E is the integral ideal or positive divisor given by

$$N(E/k) = \prod_{v \nmid \infty} \mathfrak{p}_v^{f_v},$$

where

$$f_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v \\ 1 & \text{if } E \text{ has multiplicative reduction at } v \\ 2+\delta_v & \text{if } E \text{ has additive reduction at } v, \end{cases} \tag{8}$$

and where δ_v is a non-negative integer depending on the action of wild inertia at v on $T_l E$. It is zero whenever the characteristic of v is prime to 6.

Remark. In fact, the conductor of E is the Artin conductor of the Tate module of E [45]. It is related to $\mathcal{D}(E/k)$ by Ogg's formula [41]

$$f_v = \mathrm{ord}_v(\mathcal{D}(E/k)) + 1 - m_v,$$

where m_v is the number of irreducible components of the Néron model of E at v.

We can now define the L-function.

Definition 16. The *L-function* of E/k is

$$L(E/k, s) = \prod_{v \nmid \infty} L_v(E/k, s). \tag{9}$$

When k is a number field, we also add factors at the infinite places, setting

$$\Lambda(E/k, s) = \big((2\pi)^{-s}\Gamma(s)\big)^{[k:\mathbb{Q}]} L(E/k, s),$$

whereas when k is a function field we set

$$\Lambda(E/k, s) = L(E/k, s).$$

As we saw above, the product defining $L(E/k, s)$ converges absolutely in the region $\mathrm{Re}(s) > 3/2$. In the function field case, the L-function of a constant elliptic curves will have a pole on the line $\mathrm{Re}(s) = 3/2$. We illustrate this with a specific example.

Definition 17. Let E/k be an elliptic curve over a function field $k = \mathbb{F}_q(X)$, where X is a geometrically irreducible, non-singular projective curve over $\mathbb{F}_q$. We say that E is a *constant* elliptic curve if it arises by extension of scalars from $\mathbb{F}_q$ to k, that is,

$$E = A \times_{\mathbb{F}_q} k$$

for some elliptic curve $A/\mathbb{F}_q$. Otherwise, we say that E is *non-constant.*

Example. Let $A/\mathbb{F}_4$ be the elliptic curve over the field of four elements defined by the generalized Weierstrass equation

$$A : y^2 + y = x^3 + w, \qquad \text{where } w^3 = 1, w \neq 1.$$

Our aim is to compute the L-function $L(E/k, s)$ where $k = \mathbb{F}_4(t)$ and $E = A \times_{\mathbb{F}_4} k$.

One may quickly verify that $\#A(\mathbb{F}_4) = 1$, so that its L-factor is

$$L(A/\mathbb{F}_4, s) = (1 - 4 \cdot 4^{-s} + 4 \cdot 4^{-2s})^{-1}.$$

By Theorem 11, the L-factor for A taken over the unique extension $\mathbb{F}_{4^n}/\mathbb{F}_4$ of degree n is

$$L(A/\mathbb{F}_{4^n}, s) = (1 - 2 \cdot 2^n \cdot 4^{-s} + 4^n \cdot 4^{-2s})^{-1} = (1 - 4^{-n(s-1/2)})^{-2}. \tag{10}$$

The L-function $L(E/k, s)$ is by definition the product of the local L-factors at the places of k, all of which are of good reduction. Hence

$$L(E/k, s) = Z(s - (1/2))^2$$

where $Z(s)$ is the zeta-function of the global field $k = \mathbb{F}_4(t)$. Since $X = \mathbb{P}^1$ in this case, we have

$$Z(s) = \frac{1}{(1 - 4^{-s})(1 - 4^{1-s})}$$

which has simple poles at the points $s = 0$ and $s = 1$. Hence $L(E/k, s)$ has double poles at the points $s = 1/2$ and $s = 3/2$.

Conjecture 18. *The complex analytic function $\Lambda(E/k, s)$ on the right half plane $\mathrm{Re}(s) > 3/2$ admits an meromorphic continuation to the entire complex plane and satisfies the functional equation*

$$\Lambda(E/k, s) = \pm A^{1-s} \Lambda(E/k, 2 - s), \tag{11}$$

where A is a positive integer. If E is not a constant elliptic curve, then the continuation is holomorphic.

Grothendieck proved this conjecture in the case that k is a function field; in this case it is a consequence of Poincaré duality in étale cohomology [26]. Wiles, Taylor, and others proved it in the case that $k = \mathbb{Q}$ [56], [53], [4], as a consequence of the modularity of elliptic curves over $\mathbb{Q}$. Some other cases when k is a totally real number field are known.

Remark. In the number field case, the constant A should be equal to the product of the absolute norm of $N(E/k)$ with the square of the discriminant of k. In the function field case, $A = q^{(\deg N(E/k) + 4g - 4)}$ where q is the cardinality of the constant field and g is the genus of the base curve X. Note that A corresponds with the degree of the L-function (see Proposition 22).

Remark. If Conjecture 18 is true, then the sign $\pm$ in the functional equation, which is known in general as a *root number*, is given by

$$\pm = (-1)^{\mathrm{ord}_{s=1} L(E/k, s)}, \tag{12}$$

since the reflection point of the functional equation is $s = 1$. We note that the global sign is a product of local root numbers, almost all of which are equal to $+1$ [24].

An overview of the topics of this section, with further references, may be found in [47], §C.16.

Periods. We continue with the notations of the previous section. The conjecture of Birch and Swinnerton-Dyer connects the behavior of $L(E/k, s)$ near the point $s = 1$ to the rank of $E(k)$, and to some further arithmetic invariants of E. In the previous lecture, we defined several of these invariants, namely the Tate-Shafarevitch group $Ш(k, E)$ and the regulator $R(E/k)$. It remains to define the global period of E. We begin with some motivation.

For the moment, let us assume that our L-function has a meromorphic continuation to all of $\mathbb{C}$, and consider which arithmetic properties of E might influence the behaviour of the L-function near $s = 1$. Equation (7) suggests that larger point counts at finite places would make the L-function smaller near $s = 1$. We want to put this data together, despite the fact that the infinite product

$$L(E/k, s) = \prod_{v \nmid \infty} L_v(s)$$

need not converge at the point $s = 1$. We will do this via adelic integration, a byproduct of which will be the period. For an introduction to adelic integration, see [55].

Recall that an elliptic curve has an invariant differential that is unique up to scalar multiple. For each place v of k let ω_v be a non-zero invariant differential for E/k_v. Together with the choice of a Haar measure dx_v on the additive group of k_v, this gives us a Haar measure $|\omega_v|$ on the compact group $E(k_v)$.

Lemma 19 (Tate [49]). *Let E be an elliptic curve over k_v where v is a finite place of k, and choose a minimal Weierstrass model for E. Let ω_v be an invariant differential, defined over A_v, which does not vanish modulo $\pi_v A_v$, and let dx_v be the Haar measure on k_v which gives A_v volume 1. Then*

$$\int_{E(k_v)} |\omega_v| = \frac{[E(k_v) : E^0(k_v)]}{L_v(1)}.$$

Proof. We begin with some notation. We may assume that E is given by a minimal equation

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

and that the differential is of the form

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

We let $z = -x/y$. Then z is a local parameter at the point at the point $\mathcal{O}_E$, and working in the formal completion at the origin gives that $dz = \omega_v(1 + O(z))$.

The proof of the lemma is based on the existence of the formal group of E, alluded to in the proof of the Proposition 7. Completing along the origin $z = 0$ of E gives a formal group F with the property that $(\pi_v)_F$ (that is, the set $\pi_v A_v$ endowed with the group law defined by F) is isomorphic to $E^1(k_v)$. In particular, viewing $E(k_v)$ as a v-adic analytic manifold, $z : E^1(k_v) \to \pi_v A_v$ forms a chart. It follows that

$$\int_{E^1(k_v)} |\omega_v| = \int_{\pi_v A_v} |dz(1 + O(z)| = \frac{1}{[A_v : \pi_v A_v]} \int_{A_v} |dz| = \frac{1}{q_v},$$

using the translation invariance of Haar measure and the fact that $|1 + O(z)| = 1$ when $z \in \pi_v A_v$, by the ultrametric property of the v-adic absolute value.

Write

$$N_v = [E^0(k_v) : E^1(k_v)] = \#\widetilde{E}_v^{\mathrm{ns}}(\mathbb{F}_v).$$

Applying the translation invariance of ω_v now gives

$$\int_{E(k_v)} |\omega_v| = \frac{[E(k_v) : E^0(k_v)] N_v}{q_v},$$

and re-arranging gives the result. □

Choose a non-zero invariant differential ω on E/k; it gives an invariant differential which we denote ω_v on E/k_v for all places v. Also, choose a decomposition

$$dx = \otimes_v dx_v \tag{13}$$

of the Haar measure dx on the adèles $\mathbb{A}$ of k with $\int_{\mathbb{A}/k} dx = 1$ (so dx_v is a Haar measure on k_v).

Definition 20. The *period* of E/k is

$$P(E/k) = P(\omega) = \prod_{v|\infty} \left(L_v(1) \cdot \int_{E(k_v)} |\omega_v| \right) \cdot \prod_{v|\infty} \int_{E(k_v)} |\omega_v|.$$

To see that this quantity is well defined we make the following observations: first, the conditions of Lemma 19 are satisfied for almost all finite v, that is, $\int_{A_v} dx_v = 1$, ω_v is defined over A_v, and ω_v does not vanish modulo π_v. Second, we note that $E^0 \neq E$ for only finitely many finite places v, so that by Lemma 19 the product defining $P(E/k)$ has almost all terms equal to 1.

It remains to show that the period is independent of the choice of invariant differential. This is the case, because a rescaling $\omega \mapsto \lambda\omega$ by $\lambda \in k^\times$ modifies P by a factor of

$$\prod_v |\lambda|_v = 1,$$

by the product formula. Therefore $P(E/k)$ is an invariant of the elliptic curve E/k.

Remark. The observations above amount to an introduction to adelic integration in the particular case of an elliptic curve. In this setting the $L_v(1)$ play the role of the "convergence factors" of [55], Ch. 2.

Example. Let k be a number field. If there exists a Néron differential ω over the ring of integers A of k, which has non-zero reduction modulo every prime, then

$$P(E/k) = \prod_{v|\infty} \int_{E(k_v)} |\omega|_v \cdot \prod_{v \text{ bad}} [E(k_v) : E^0(k_v)] \cdot |D_k|^{-1/2}, \tag{14}$$

where D_k is the discriminant of k. The discriminant appears because (with the usual local normalization of dx_v at every place) the compact quotient $\mathbb{A}/k$ has volume $|D_k|^{1/2}$ ([55], §2.1.3).

Example. Let k be a function field of genus g, with constant field $\mathbb{F}_q$. Then

$$P(E/k) = \prod_{\text{bad } v} [E(k_v) : E^0(k_v)] / \left(q^{g-1+\frac{1}{12}\deg \mathcal{D}(E/k)}\right). \tag{15}$$

For comparison with the number field case, the factor $q^{-(g-1)}$ reflects the volume $\int_{\mathbb{A}/k} dx = q^{g-1}$ of $\mathbb{A}/k$ under the standard product Haar measure ([55], §2.1.3), and the factor $q^{-\frac{1}{12}\deg \mathcal{D}(E/k)}$ stems from the obstruction to the existence of an everywhere integral Néron differential.

The conjecture of Birch and Swinnerton-Dyer. We now have all of the definitions in place in order to state the precise form of the Birch and Swinnerton-Dyer conjecture.

Conjecture 21. *Let E/k be an elliptic curve over a global field, and assume that $L(E/k, s)$ has a meromorphic continuation to a neighborhood of the point $s = 1$.*

(1) *If n is the rank of the finitely generated abelian group $E(k)$, then*

$$\operatorname{ord}_{s=1} L(E/k, s) = n.$$

(2) *Set* $c(E/k) = P(E/k) \cdot R(E/k) \cdot \#Ш(k, E)$. *Then*

$$L(E/k, s) \sim c(E/k) \cdot (s-1)^n \text{ as } s \to 1.$$

For another discussion of this conjecture, with a reward attached, see [57].

A naïve original motivation for this conjecture is that one might expect a larger number of rational points to yield larger numbers of points on reductions modulo finite places. Then the partial products of the infinite product

$$L_S(E/k, 1) \text{“} = \text{”} \prod_{\text{good } v} L_v(E/k, 1) = q_v / \#\widetilde{E}_v(\mathbb{F}_v)$$

would tend to be relatively smaller. The original conjecture and the numerical evidence that led to it are recorded in [2].

Remark. A much weaker form of Conjecture 21 is the parity conjecture, that $\pm$, the sign of the functional equation of E is equal to $(-1)^{\text{rank}(E(k))}$. Compare the remark after Conjecture 18.

Remark. We have seen that the L-function is an isogeny invariant of E/k. The individual terms $P(E/k)$, $R(E/k)$, and $\#Ш(k, E)$ which occur in the conjecture of Birch and Swinnerton-Dyer are isomorphism invariants, and can change when we modify E by an isogeny. However, their product is an isogeny invariant [8], [52], [38].

Remark. Bloch [3] defines an extension of commutative algebraic groups

$$1 \longrightarrow \mathbb{G}_m^n \longrightarrow G \longrightarrow E \longrightarrow 1$$

over k, where n is the rank of $E(k)$. The existence of such an extension is a consequence of the theorem of Serre-Rosenlicht [44], VII, Thm. 6, which gives a natural isomorphism between the groups $\text{Ext}_k(E, \mathbb{G}_m)$ and $\text{Pic}^0(E)(k)$, the latter being naturally identified with the k-rational points of E.

The L-function for G is the product

$$L(G/k, s) = L(E/k, s)\zeta_k(s)^n,$$

where $\zeta_k(s)$ is the Dedekind zeta-function of k. Therefore we expect $L(G/k, s)$ to be regular and non-zero at $s = 1$. Bloch shows that $G(k)$ is discrete and co-compact in $G(\mathbb{A})$, where $\mathbb{A}$ is the ring of adeles of k, and calculates the volume of the quotient group $G(\mathbb{A})/G(k)$ in terms of the period and regulator of E/k. He shows that the Birch and Swinnerton-Dyer conjecture for E would follow from standard conjectures on Tamagawa numbers, applied to the algebraic group G.

Examples of elliptic curves over number fields.

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

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

of conductor $N = 37$. We will calculate some of the invariants of E to show what the Birch and Swinnerton-Dyer conjecture implies.

Let v be a place of good reduction. By Proposition 7, the reduction map $E(\mathbb{Q}) \to \widetilde{E}(\mathbb{F}_v)$ is injective on n-torsion when n is prime to v. In this case we have

$$\#\widetilde{E}(\mathbb{F}_2) = 5 \text{ and } \#\widetilde{E}(\mathbb{F}_3) = 7,$$

and so $E(\mathbb{Q})$ is torsion-free. Since $P = (0,0) \in E(\mathbb{Q})$ is not equal to $\mathcal{O}_E$, the rank of E over $\mathbb{Q}$ must be at least one. In fact, one can check that $E(\mathbb{Q}) = \mathbb{Z}P$ via a descent argument similar to the one outlined in the previous lecture.

Next, we will calculate the period of E. The Tamagawa factors $[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ are trivial at all places of good reduction, and applying Tate's algorithm and looking at the table in [49], noting that E has multiplicative reduction at 37 with $\mathrm{ord}_{37}(j(E)) = -1$, shows that $E = E^0$ at $p = 37$ as well. Equation (14) now gives $P(E/k) = \int_{E(\mathbb{R})} |\omega|$. The BSD conjecture predicts that $L(E/\mathbb{Q}, 1) = 0$ and

$$L'(E/\mathbb{Q}, 1) = \#Ш(\mathbb{Q}, E) \cdot \langle P, P \rangle \cdot \int_{E(\mathbb{R})} |\omega|, \tag{16}$$

where ω is a Néron differential on $E/\mathbb{Q}$.

The sign in the functional equaltion of $L(E/\mathbb{Q}, s)$ is equal to -1, so the L-function vanishes to odd order at $s = 1$. One can compute the value $L'(E/\mathbb{Q}, 1)$, which is non-zero. Hence the L-function vanishes to order exactly 1, i.e. E has analytic rank 1. Via the work of Kolyvagin [31] and Gross-Zagier [25], the Birch and Swinnerton-Dyer conjecture is known for curves of analytic rank 0 and 1, up to some ambiguity in the leading term. In this case, the full conjecture is known to be true. We have

$$L'(E/\mathbb{Q}, 1) = \langle P, P \rangle \cdot \int_{E(\mathbb{R})} |\omega|$$

and the group $Ш(\mathbb{Q}, E)$ is trivial.

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

$$E : y^2 + y = x^3 - 7x + 6, \tag{17}$$

of conductor $N = 5077$. Brumer and Kramer found that this is the elliptic curve over $\mathbb{Q}$ of rank 3 with smallest conductor, making it an

interesting case study for elliptic curves of higher rank. (It also has 36 points with integral coordinates in the minimal model.) It has no non-trival torsion because its reductions modulo 2 and 3 are the same as in the above example. Also, as in the previous example, $E(\mathbb{Q}_p) = E^0(\mathbb{Q}_p)$ for all p because $\mathrm{ord}_{5077}(j(E)) = -1$.

In [6] the authors make a detailed study of the invariants of E, which together with the conjecture of Birch and Swinnerton-Dyer would imply that $Ш(\mathbb{Q}, E) = 1$. We now review these computations. Via a descent and height calculations, one can show that $P_1 = (0, 2), P_2 = (1, 0), P_3 = (2, 0)$ generate $E(\mathbb{Q})$, i.e.

$$E(\mathbb{Q}) = \mathbb{Z}P_1 + \mathbb{Z}P_2 + \mathbb{Z}P_3.$$

A calculation of the real period $\int_{E(\mathbb{R})} |\omega|$, the regulator $R(E/\mathbb{Q})$, and the L-function around $s = 1$ suggests that that $L(E/\mathbb{Q}, s)$ vanishes to order 3 around $s = 1$ with leading term

$$c(E/k) \approx R(E/\mathbb{Q}) \cdot \int_{E(\mathbb{R})} |\omega| = 1.73185\ldots,$$

accurate to 28 decimal places. Although this calculation suggests strongly that $Ш(\mathbb{Q}, E)$ is trivial, we still don't know if it is finite.

Remark. These examples of elliptic curves with rank 3 were important in finding the first effective lower bound on class numbers of positive definite binary quadratic forms, completing the program of Goldfeld [21], [20]. Namely, the Gross-Zagier formula [25] implies that for an elliptic curve $E/\mathbb{Q}$ whose L-function has a odd-order zero at $s = 1$, there exists a computable point $P \in E(\mathbb{Q})$ such that

$$L'(E/\mathbb{Q}, 1) = c\langle P, P\rangle,$$

where c is a positive constant. If the point P is torsion (hence $\langle P, P\rangle = 0$) the derivative vanishes. This argument applied to the elliptic curve defined in equation (17) allows one to show that $L(E/\mathbb{Q}, s)$ vanishes to order 3 at $s = 1$.

L-functions of elliptic curves over function fields. Let k be the function field of an irreducible non-singular projective curve X of genus g over the finite field $\mathbb{F}_q$ of q elements. We will assume that $\overline{\mathbb{F}}_q \cap k = \mathbb{F}_q$, or equivalently that X is geometrically irreducible (cf. [32], Cor. 3.2.14).

Proposition 22. *Let E/k be an elliptic curve. Then we can write*

$$L(E/k, s) = M(q^{-s})$$

where $M(x)$ is a rational function of degree

$$\deg M = 4g - 4 + \deg N(E/k). \tag{18}$$

If E/k is non-constant, then $M(x)$ is a polynomial with integer coefficients, and constant coefficient equal to 1.

The proof uses étale cohomology, cf. [11], [37]. The L-functions of elliptic curves can be expressed in terms of characteristic polynomials of Frobenius actions on appropriate étale cohomology groups.

Definition 23. Let U be a geometrically irreducible non-singular curve over $\mathbb{F}_q$. Let X be the (unique) non-singular completion of U, cf. [28] I.6. Then $k = \mathbb{F}_q(U) = \mathbb{F}_q(X)$. Write S for the set of places of k which correspond to points of $X - U$, and let K_S be the maximal separable extension of k which is unramified outside S, inside a suitable separable closure of k. We call the group $\mathrm{Gal}(K_S/k)$ the *étale fundamental group* $\pi_1(U)$ of U. Let l be a prime not dividing q. A *lisse l-adic sheaf* $\mathcal{F}$ on U is a continuous finite-dimensional l-adic representation of $\pi_1(U)$.

We have adopted a simplified definition here in order to avoid unnecessary complications. For the general definition, we refer to [27] or [37]. As examples of lisse l-adic sheaves, we have the trivial representation $\mathbb{Q}_l$ of $\pi_1(X)$, and the representation $V_l(E)$ of $\pi_1(U)$, where E is an elliptic curve over $k = \mathbb{F}_q(X)$ and U is the complement of the set S of places of bad reduction. By the criterion of Néron-Ogg-Shafarevitch [45], this representation is unramified at places of good reduction, hence it is lisse on U. In Grothendieck's theory, we will often work with the dual representation $V_l E^\vee$ of $\pi_1(U)$, which is the cohomology in degree 1 of the family of curves over U. The Weil pairing gives an isomorphism with the Tate twist

$$V_l(E)^\vee \cong V_l(E)(-1).$$

We note that the arithmetic Frobenius $\phi : x \mapsto x^q$ in the Galois group acts by the scalar q on $\mathbb{Q}_l(1)$, so the geometric Frobenius $\mathrm{Frob} = \phi^{-1}$ acts by q on the twist $\mathbb{Q}_l(-1)$.

Definition 24. Let $\mathcal{F}$ be a lisse l-adic étale sheaf on a non-singular geometrically irreducible curve $U/\mathbb{F}_q$, and let U^0 denote the set of closed points of U. Then the *formal L-function of $\mathcal{F}$* is given by

$$L(U, \mathcal{F}, t) = \prod_{y \in U^0} \det\left(1 - t^{\deg y}\,\mathrm{Frob}_y \mid \mathcal{F}\right).$$

Here Frob_y denotes the geometric Frobenius at the place v corresponding to y.The L-function $L(U, \mathcal{F}, s)$ is given by substituting q^{-s} for t.

Let us now sketch the proof of Proposition 22. In order to avoid technical complications we will make some simplifying assumptions along the way. For example, we will assume that q is not a power of 2 or 3 to avoid dealing with wild ramification.

Proof. **Step 1: The bad factors.** Let S be the set of places of bad reduction of E/k. We have

$$L(E/k,s) = \prod_v L_v(E/k,s) = L_S(E/k,s) \cdot \prod_{v \in S} L_v(E/k,s).$$

First we will discuss the latter factor, coming from places of bad reduction. Recall the L-factors at places of bad reduction, given in Equation (6), and compare them to the formula for the conductor $N(E/k)$ of E given in Definition 15. Our assumption on q implies that the factors δ_v in Equation (8) vanish, hence

$$\prod_{v \in S} L_v(E/k,t) \text{ is a rational function of degree } \deg N(E/k) - 2 \cdot \#S.$$

To complete the proof, it suffices to show that the first factor $L_S(E/k,t)$ is a rational function of degree $4g - 4 + 2 \cdot \#S$.

Step 2. An equality of L-functions. Write U for the complement of S in X, and consider $V_l E$ as a representation of the étale fundamental group $\pi_1(U)$, i.e. as a lisse l-adic étale sheaf on U. Therefore, by the equality of the characteristic polynomial of $\rho_{E,l}(\phi_v)$ in Equation (4) with the definition of an L-factor in Equation (2), one obtains an identity of L-functions

$$L_S(E/k,t) = L(U, V_l E^\vee, t).$$

where $V_l E^\vee$ is the dual representation, on the first degree cohomology of E.

Step 3: Grothendieck's work on L-functions In this step we split into two cases, depending on whether the set S of places of bad reduction is empty or not. A good general reference on this material is [29].

Case $S \neq \emptyset$. The curve U is affine since S is not empty, and $V_l E$ is lisse. These conditions imply, by a version of the Lefschetz trace formula [37], that

$$L(U, V_l E^\vee, t) = \frac{\det(1 - t\,\mathrm{Frob} \mid H^1_c(U \times_{\mathbf{F}_q} \overline{\mathbb{F}}_q, V_l E^\vee))}{\det(1 - t\,\mathrm{Frob} \mid H^2_c(U \times_{\mathbf{F}_q} \overline{\mathbb{F}}_q, V_l E^\vee))},$$

where the cohomology is étale cohomology with compact supports. Here Frob continues to denote the geometric Frobenius. The denominator is trivial, because $H^2_c(V_lE^\vee) = 0$. Indeed, it is Poincaré dual to $H^0(V_lE)(-1)$. But the group $H^0(V_lE)$ is equal to the invariants of $\mathrm{Gal}(k^s/\overline{\mathbb{F}}_q(X))$ on V_lE. Since E/k is non-constant, there are only a finite number of l- torsion points defined over $\overline{\mathbb{F}}_q(X)$, and this group is trivial.

The cohomology with compact supports on an affine curve always vanishes in all degrees not 1 or 2. We have shown that it is also trivial in degree 2 in this case. Hence the rank of $H^1_c(U \times_{\mathbf{F}_q} \overline{\mathbb{F}}_q, V_lE^\vee)$ is the negative of the Euler characteristic of this cohomology. We have shown that $L_S(E/k,t)$ is a polynomial. To show that its degree is equal to $4g-4+2\#S$ it remains to show that the Euler characteristic $\chi(H^*(U,V_lE^\vee))$ is equal to $4-4g-2\#S$. We can calculate this Euler characteristic using use ordinary étale cohomology, which is Poincaré dual to cohomology with compact supports.

Case $S = \emptyset$. In this case $X = U$. For a lisse étale sheaf over the smooth geometrically irreducible projective curve X, the determination of the L-function is even more straightforward because as $X/\mathbb{F}_q$ is proper, there is no concern with compact supports. Grothendieck's theory implies that

$$L(X, V_lE^\vee, t) = \prod_{0\le i\le 2} \det(1 - t\,\mathrm{Frob} \mid H^i(X \times_{\mathbf{F}_q} \overline{\mathbb{F}}_q, V_lE^\vee))^{-(-1)^i}$$

Therefore it again suffices to show that the Euler characteristic of the étale cohomology of $V_lE^\vee$ is $4-4g$.

Step 4: Raynaud's Euler Characteristic Formula. This formula, given in [42], gives the Euler characteristic of the cohomology of l-adic sheaves as the product of the Euler characteristic of the base U with the rank of the sheaf, modified by terms that measure the wild ramification at points in S. There is no wild ramification on X in our case, because we have assumed that q is not a power of 2 or 3. Thus

$$\chi(H^*(U, V_lE^\vee)) = \chi(U) \cdot \dim_{\mathbf{Q}_l} V_lE^\vee.$$

As we saw above, $V_lE^\vee$ is of dimension 2 and the Euler characteristic of U is given by $\chi(X) - \#S = 2 - 2g - \#S$. This shows that $\chi(H^*(U, V_lE^\vee)) = 4 - 4g - 2\#S$, which is what was needed in both of the cases in Step 3. □

Remark. Assume that E is constant, $E = A \times_{\mathbf{F}_q} X$ for some an elliptic curve $A/\mathbb{F}_q$. If Y is a smooth projective variety over $\mathbb{F}_q$ of dimension

d, we can define its zeta function as

$$Z(Y,t) = \prod_{y \in Y^0} (1 - t^{\deg y}) = L(Y, \mathbb{Q}_l, t), \tag{19}$$

which by the Lefschetz trace formula [26] is equal to

$$Z(Y,t) = \prod_{i=0}^{2d} \det(1 - t\,\mathrm{Frob} \mid H^i(Y, \mathbb{Q}_l))^{(-1)^{i+1}}$$

In particular, we find that

$$Z(A,t) = \frac{1 - at + qt^2}{(1-t)(1-qt)} = \frac{L_v(E/k,t)^{-1}}{(1-t)(1-qt)}$$

where $a = q + 1 - \#A(\mathbb{F}_q)$ and

$$Z(X,t) = \frac{M(t)}{(1-t)(1-qt)}$$

where $M(t)$ is a polynomial of degree $2g(X)$. By the Künneth formula and the general relation between zeta and L-functions

$$L(E/k,t) = \frac{\det(1 - t\,\mathrm{Frob} \mid H^1(A) \otimes H^1(X))}{\det(1 - t\,\mathrm{Frob} \mid (H^1(A) \otimes H^0(X)) \oplus (H^1(A) \otimes H^2(X)))}.$$

As the Frobenius eigenvalues on the 1-dimensional $\mathbb{Q}_l$-vector spaces $H^0(X)$ and $H^2(X)$ are 1 and q respectively, we find that

$$L(E/k,s) = \frac{\det(1 - t\,\mathrm{Frob} \mid H^1(A) \otimes H^1(X))}{(1 - aq^{-s} + q^{1-2s})(1 - aq^{1-s} + q^{3-2s})} \tag{20}$$

Note that this is a rational function of degree $4g-4$ in q^{-s} as expected.

Examples of elliptic curves over function fields. We present two examples of non-constant elliptic curves where the conjecture of Birch and Swinnerton-Dyer is known to be true. In both cases, $X = \mathbb{P}^1$ and $k = \mathbb{F}_q(X) = \mathbb{F}_q(t)$.

Example. Suppose that q is odd, and consider the elliptic curve E/k given by the equation

$$y^2 = x(x-1)(x-t), \text{ of discriminant } \Delta = 16t^2(t-1)^2.$$

This is the first curve studied in the previous lecture. Making the change of variable $s = 1/t$ gives the equation

$$y^2 = x(x-s)(x-s^2), \text{ of discriminant } \Delta' = 16s^8(s-1)^2,$$

As we noted in lecture 1, a change of variable changes the valuation of the discriminant at each place by a multiple of 12; it follows that the above equations are both minimal at every place where they are

integral. We see that E has multiplicative reduction at the places $t = 0, 1$ and additive reduction at $t = \infty$, and the conductor and minimal discriminant are given by (cf. Equation 8)

$$N(E/k) = (0) + (1) + 2(\infty) \text{ and } \mathcal{D}(E/k) = 2(0) + 2(1) + 8(\infty).$$

An application of Tate's algorithm shows that the reduction at the bad places $t = 0, 1, \infty$ are of Kodaira types I_2, I_2 and I_2^* respectively [49].

To calculate the period $P(E/k)$, we need to know the quantities $\deg \mathcal{D}(E/k) = 12$, the genus $g(X) = 0$, and the indices $[E(k_v) : E^0(k_v)]$ at the places of bad reduction $t = 0, 1, \infty$, which are $2, 2$, and 4, respectively, cf. [49]. Using Equation (15), we find that

$$P(E/k) = \prod_{\text{bad } v} [E(k_v) : E^0(k_v)] = 2_0 \cdot 2_1 \cdot 4_\infty = 16.$$

To calculate the regulator $R(E/k)$, we recall from the previous lecture that

$$E(k) = \{O_E, (0,0), (1,0), (t,0)\}.$$

Hence

$$R(E/k) = \#E(k)^{-2} = 1/16.$$

Finally, since the degree of $N(E/k)$ is 4, Proposition 22 implies that $L(E/k, s) = 1$. Now, the Birch and Swinnerton-Dyer conjecture is known for this elliptic curve, since E is the generic fiber of a rational surface (cf. the next lecture). It follows that

$$1 = L(E/k, 1) = P(E/k) \cdot R_E \cdot \#Ш(k, E) = \#Ш(k, E),$$

so the Tate-Shafarevitch group is trivial. The fact that the 2-torsion in $Ш(k, E)$ is trivial follows from the descent calculation of lecture 1.

Example. Assume that $q = p$ is an odd prime. Let E'/k be the elliptic curve defined by

$$E' : t(t-1)y^2 = x(x-1)(x-t).$$

The minimal regular model of E' over X is a K3 surface over $\mathbb{F}_q$. In this case, the conjecture of Birch and Swinnerton-Dyer is also known to be true.

A similar computation to the one above reveals that

$$N(E'/k) = 2(0) + 2(1) + 2(\infty) \text{ and } \mathcal{D}(E'/k) = 8(0) + 8(1) + 8(\infty).$$

Proposition 22 then implies that $L(E'/k, s)$ is a polynomial of degree 2 in p^{-s}. After a calculation (cf. section 8.8 of [30]) one finds that this polynomial is

$$L(E'/k, s) = \begin{cases} 1 - 2(a^2 - b^2)p^{-s} + p^{2-2s} & \text{if } p \equiv 1 \pmod 4; \\ 1 - p^{2-2s} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where a, b are the unique positive integers such that a is odd and $p = a^2 + b^2$.

In the case that $p \equiv 1 \pmod 4$, we get

$$L(E'/k, 1) = (1 - 2(a^2 - b^2)/p + 1) = 4b^2/p \neq 0.$$

Proceding as before, Equation (15) implies that $P(E'/k) = 4 \cdot 4 \cdot 4/p$ since $[E'(k_v) : E'^0(k_v)] = 4$ at the places $t = 0, 1$, and ∞, and $\deg \mathcal{D}(E'/k) = 24$. Since the L-function does not vanish at $s = 1$ we know that $E'(k)$ is finite, and is an easy matter to compute the torsion subgroup, showing that $\#E'(k) = 4$, and hence that we have $R(E'/k) = 1/4^2$. Then the Birch and Swinnerton-Dyer conjecture implies that

$$\#Ш(k, E') = b^2.$$

Since b is even, we see that $Ш(k, E')$ is non-trivial. The fact that $Ш(k, E')$ has even order is consistent with the descent calculation in lecture 1.

In the case that $p \equiv 3 \pmod 4$, $L(E'/k, 1) = 0$ and $L'(E'/k, 1) = 2 \log p$, so by the Birch and Swinnerton-Dyer conjecture $E'(k)$ has rank exactly 1. As before, $P(E'/k) = 64/p$. If we take P to be a generator modulo torsion then $E'(k) = \mathbb{Z}P + (\mathbb{Z}/2\mathbb{Z})^2$, so

$$R(E/k) = \langle P, P \rangle / 4^2,$$

which as we mentioned at the end of the previous lecture is equal to $r \log p/4^2$ where r is rational. In fact $r \in \frac{1}{2}\mathbb{Z}$; the height pairing takes on integral values except for contributions from places of bad reduction, the denominators of which can be bounded explicitly in terms of the Kodaira type, cf. lecture 3.

Applying the Birch and Swinnerton-Dyer conjecture, we see that

$$2 \log p = L'(E/k, 1) = c(E/k) = 4r \log p \#Ш(k, E),$$

so $\#Ш(k, E) \cdot 2r = 1$. The existence of the Cassels-Tate pairing (cf. [7], [52]) implies that $Ш(k, E)$ has square order, and consequently that $\#Ш(k, E) = 1$ and $r = \frac{1}{2}$.

Lecture 3: Progress to date

Results over number fields. Let k be a number field, and E/k an elliptic curve. As we saw in lecture 2, the conjecture of Birch and Swinnerton-Dyer cannot be formulated until one knows that the L-function of E/k can be analytically continued to a neighborhood of the point $s = 1$. This continuation has been established for some elliptic curves, which we now describe.

A Shimura curve X over $\mathbb{C}$ is the quotient of the upper half plane by an arithmetic Fuchsian group. These groups all arise from quaternion algebras over totally real number fields k, which are split at precisely one real place v of k. The associated system of Shimura curves has a canonical model over the field k, embedded in $\mathbb{C}$ via the place v [12], [13], [58].

Definition 25. We say an elliptic curve E over a totally real number field k is *modular* if it is isogenous over k to a factor of the Jacobian of some Shimura curve.

When $k = \mathbb{Q}$, it is known that all elliptic curves are modular [4]. Here one only needs the classical modular curves, which are the Shimura curves associated to the split quaternion algebra of two-by-two matrices over $\mathbb{Q}$.

Theorem 26 (Gross-Zagier [25], Kolyvagin [31], Zhang [58]). *Let E/k be a modular elliptic curve over the totally real number field k. Then $L(E/k, s)$ is entire and satisfies Conjecture 18. If we assume further that $\mathrm{ord}_{s=1} L(E/k, s) \leq 1$, then*

(1) $\mathrm{rank}(E(k)) = \mathrm{ord}_{s=1} L(E/k, s)$;
(2) $Ш(k, E)$ *is finite; and*
(3) *the Birch and Swinnerton-Dyer conjecture is true at almost all primes.*

This theorem is due to Gross-Zagier and Kolyvagin for $k = \mathbb{Q}$ and to Zhang in the general case. By the statement "is true at almost all primes", we mean that the ratio $c(E/k)/(R(E/k) \cdot P(E/k))$ is a non-zero rational number. and that for all rational primes p outside of a specified finite set depending on the curve E, the p-part of the order of $Ш(k, E)$ is equal to the p-part of this ratio. In many cases, one can refine Kolyvagin's method to prove that the specified finite set is empty.

The crux of the proof is the exploitation of special points on Shimura curves, which are defined over abelian extensions of CM fields K with totally real subfield k. We give a sketch in the case that $k = \mathbb{Q}$, where the special points are called *Heegner points*. Assume that E has conductor $N = N(E/\mathbb{Q})$. Then the proof that E is modular exhibits a weight 2 newform f for the group $\Gamma_0(N)$ with integer Fourier coefficients such that $L(f, s) = L(E/\mathbb{Q}, s)$. The space of cusp forms of weight 2 for $\Gamma_0(N)$ is naturally identified with the space of holomorphic differentials on $X_0(N)$. This implies that E is isogenous to a quotient of the Jacobian $J_0(N)$ over $\mathbb{Q}$ [15].

The composition of the canonical map $X_0(N) \to J_0(N)$, obtained by sending the cusp ∞ to the zero point of $J_0(N)$, with the projection $J_0(N) \to E$ gives a dominant map $\pi : X_0(N) \to E$ defined over $\mathbb{Q}$. We let ω be the unique invariant differential on E over $\mathbb{Q}$ which satisfies $\pi^*(\omega) = \omega_f = 2\pi i f dz$ [33].

The complement of the cusps in $X_0(N)$ is a coarse moduli space of elliptic curves (A, A') related by a cyclic N-isogeny. Let K be an imaginary quadratic number field of discriminant D in which all the prime factors of N are split. There exists an integral ideal $\mathfrak{n}$ of K such that $\gcd(\mathfrak{n}, \bar{\mathfrak{n}}) = 1$ and $\mathfrak{n} \cdot \bar{\mathfrak{n}} = (N)$, and the complex elliptic curves given by the lattice quotients $A = \mathbb{C}/\mathfrak{n}$ and $A' = \mathbb{C}/\mathcal{O}_K$ are related by the isogeny $x : A \to A'$ with cyclic kernel $\mathcal{O}_K/\mathfrak{n}$ of order N. By the theory of complex multiplication, cf. [48], Ch. II, this Heegner point x is defined over the Hilbert class field H of K, that is, $x \in X_0(N)(H)$.

Recall that $\pi(x)$ is the projection of the class $[x] - [\infty] \in J_0(N)(H)$ to $E(H)$, and let

$$P = \sum_{\sigma \in \mathrm{Gal}(H/K)} \pi(x)^\sigma \in E(K),$$

the addition occurring in $E(H)$. Birch asked when P had infinite order in the group $E(K)$. Based on extensive computations, he conjectured that this question was related to the non-vanishing of the first derivative of $L(E/K, s)$ at $s = 1$. It is proved in [25] that

$$L'(E/K, s) = \frac{\langle P, P \rangle_K}{\sqrt{|D|}} \cdot \int_{E(\mathbb{C})} |\omega|.$$

The proof of this identity follows from a comparison of the calculation of the first derivative, using Rankin's integral formula for the L-function, with the calculation of the global height of P, using Néron's theory of local heights on the curve $X_0(N)$, discussed below.

In particular, P has infinite order if and only if $L'(E/K, 1)$ does not vanish. If P has infinite order, Kolyvagin's work then shows that $Ш(K, E)$ is finite. Combining this argument with some non-vanishing results for the L-series of quadratic twists gives the result in the theorem when

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

is 0 or 1. This completes our sketch of the proof.

Local and global heights. Let k be a global field. Néron's theory of local heights (cf. [40], [25]) expresses the canonical height pairing on

the Jacobian J of a curve X/k as a sum

$$\langle \alpha, \beta \rangle = \sum_{\text{places } v} \langle a, b \rangle_v$$

of local terms, almost all of which are zero. Here we take a, b to be divisors of degree zero on X with disjoint supports representing the classes α and β. The local symbols $\langle , \rangle_v$ are characterised by the property that they are bi-additive, symmetric, continuous, and satisfy

$$\langle a, \operatorname{div}(f) \rangle_v = \log |f(a)|_v = \log \prod_x |f(x)|_v^{m_x},$$

where $a = \sum_x m_x \cdot x$ and f is a rational function on X.

When v is archimedean, the local height pairing $\langle , \rangle_v$ is defined using potential theory. When v is a non-archimedean place, the local pairing can be defined using intersection theory as follows. Let $\mathcal{E}$ be the minimal regular model of E over $\operatorname{Spec} A_v$, cf. [10], [32].

We write $\mathcal{F} = \sum a_i \mathcal{F}_i$, where $\mathcal{F}$ is the special fiber of $\mathcal{E}$, the $\mathcal{F}_i$ are its irreducible components, and the a_i are their respective multiplicities. The intersection pairing $(,)$ in the special fiber has the property that $(\mathcal{F}, \mathcal{F}_i)$ is zero for each i. Furthermore, it is negative definite on the quotient group $\sum_i \mathbb{Z}\mathcal{F}_i / \mathbb{Z}\mathcal{F}$, so is non-degenerate over $\mathbb{Q}$.

To define the local height in this case, take a divisor $a = \sum m_x \cdot x$ on E of degree 0, and its closure A in $\mathcal{E}$. It suffices to treat the case that a is pointwise rational over k_v (i.e. if $m_x \neq 0$, then x has co-ordinates in k_v).

By the non-degeneracy of the intersection pairing in the special fiber, we can find a $\mathbb{Q}$-divisor μ, whose support lies in the special fiber, such that $(A - \mu, \mathcal{F}_i) = 0$ for each i. Given a degree 0 divisor b, rational over k_v, relatively prime to a, we take its closure B in $\mathcal{E}$, and define

$$\langle a, b \rangle_v = (A - \mu, B) \cdot \log \#(A_v / \pi_v A_v).$$

Using the classification of the special fibers of the minimal regular models of elliptic curves, and their intersection matrices (cf. the table in [49]), one can find bounds on the denominators of the local pairing, and thus of the global height pairing for function fields. This fact was used in the previous lecture. A detailed computation of the denominators, corresponding to the classification of special fibers, can be found in [46].

Results over function fields. Let $\mathbb{F}_q$ be a finite field with $q = p^e$ elements, and X a non-singular geometrically irreducible projective curve, defined over $\mathbb{F}_q$. It follows that $\overline{\mathbb{F}}_q \cap k = \mathbb{F}_q$, where we write $k = \mathbb{F}_q(X)$ for the function field of X.

Theorem 27 (M.Artin - Tate [52]). *Let E be an elliptic curve, defined over k. Then*

$$\operatorname{ord}_{s=1} L(E/k, s) \geq \operatorname{rank} E(k),$$

and the following are equivalent:

(1) *Equality holds above.*
(2) *$Ш(k, E)$ is finite.*
(3) *$Ш(k, E)[l^\infty]$ is finite for a single prime l.*
(4) *The conjecture of Birch and Swinnerton-Dyer is true for the curve E over k.*

The curve E can be considered as the generic fiber of an elliptic surface $S/\mathbb{F}_q$ fibered over X. In this case $E(k)$ is closely connected to the *Néron-Severi group* $NS(S)$ of S. Motivated by this, Artin and Tate formulated a more general conjecture, similar in spirit to the conjecture of Birch and Swinnerton-Dyer, relating the rank of the Néron-Severi group and some other geometric invariants of a general surface S to its zeta function. In this setting, the cohomological Brauer group $H^2(S, \mathbb{G}_m)$ plays the role of the Tate-Shafarevitch group.

In [52] Tate gives the translation of the above theorem into this language and a proof of the "prime-to-p" part of the conjecturre, using l-adic étale cohomology for $l \neq p$. Milne completed the proof in [35], using more sophisticated cohomology theories capable of handling the complications at the prime p. We give a brief sketch.

We recall that for a smooth projective surface over an algebraically closed field, the Néron-Severi group is defined as the group of divisors modulo algebraic equivalence, cf. [28]. It is a finitely generated abelian group. We take S to be the minimal regular model of E over X. Then $NS(S)$ is defined to be the image of $\operatorname{Pic}(S)$ in $NS(S \otimes \overline{\mathbb{F}}_q)$. We then have injections

$$E(k) \otimes \mathbb{Q}_l \hookrightarrow NS(S) \otimes \mathbb{Q}_l \hookrightarrow H^2(S \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_l)(1),$$

the latter arrow coming from the cycle map in étale cohomology. Moreover, we have an exact sequence for every $l \neq p$:

$$0 \longrightarrow NS(S) \otimes \mathbb{Q}_l \longrightarrow (H^2(S \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_l)(1))^{G_{\mathbb{F}_q}} \longrightarrow V_l Ш(k, E) \longrightarrow 0.$$

Here $V_l Ш(k, E) = \operatorname{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, Ш(k, E)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is the analogue of the l-adic Tate module for the torsion group $Ш(k, E)$. It vanishes if and only if $Ш(k, E)[l^\infty]$ is finite. We note that the map $E(k) \otimes \mathbb{Q}_l \to NS(S) \otimes \mathbb{Q}_l$ need not be surjective, but its cokernel is well understood. In particular, there is a formula

$$\operatorname{rank} NS(S) = \operatorname{rank} E(k) + 2 + \sum_{t \in X} (m_t - 1),$$

where m_t is the number of irreducible components in the fiber above t. We refer to [46] for more details, as well as for the definition of the map $E(k) \to NS(S)$.

The zeta-function of S is given by the formula

$$\prod_i P_i(S, q^{-s})^{(-1)^{i+1}}, \text{ where } P_i(S,t) = \det(1 - \mathrm{Frob}\, q^{-s} | H^i(S, \mathbb{Q}_l)),$$

and Tate's geometric conjecture can now be rephrased in terms of the order of vanishing of $P_2(S, q^{-s})$ at $s = 1$. Looking at the above exact sequence, we see that this is equal to the multiplicity of q as an eigenvalue of Frobenius on H^2, which gives the first inequality in the theorem. Moreover, equality holds if and only if the l-primary part of the Tate-Shafarevitch group is finite. One can also show that the polynomials $P_i(S,T)$ are independent of l. These facts give the equivalence of the first 3 statements; and the equivalence of the last follows from a more involved calculation, once $Ш(k,E)$ is known to be finite.

Constant curves. We continue with the notation of the previous section, and specialize to the case where E/k is a constant curve. In this case the surface S can be taken to be $E \times_{\mathbb{F}_q} X$.

First, we note that $E(k)_{\mathrm{tors}} = E(\mathbb{F}_q)$. Indeed, the torsion points of E are defined over an algebraic extension of $\mathbb{F}_q$, and $\overline{\mathbb{F}}_q \cap k = \mathbb{F}_q$.

Next, suppose that P is a point of infinite order in $E(k)$. This point can be viewed as a section $s : X \to S$; since the section s is not constant, it induces a dominant morphism $\pi : X \to E$, of finite degree. We have the formula

$$\langle P, P \rangle = (2 \deg \pi) \log q.$$

This follows from the fact that the height pairing on $E(k)$ is induced by the intersection pairing on S.

Giving the image of P in the quotient $L = E(k)/E(F)$ is the same as giving the map π, up to translation by elements of $E(\mathbb{F}_q)$. Since the Jacobian J of X is also the Albanese variety (cf. [36]), we can identify

$$L = E(k)/E(F) = \mathrm{Hom}_{\mathbb{F}_q}(J, E).$$

We view L as an integral even lattice, that is, a free $\mathbb{Z}$-module with a positive definite integer-valued quadratic form, the form in this case being the height divided by $2 \log q$. Lattices arising in this manner are called *Mordell-Weil lattices*, and have many interesting properties. These have been studied by Elkies, Shioda and others, cf. [17], [46].

By Equation 20,

$$L(E/k, s) = \frac{\det(1 - \mathrm{Frob}\, q^{-s} | H^1(E, \mathbb{Q}_l) \otimes H^1(X, \mathbb{Q}_l))}{(1 - aq^{-s} + q^{1-2s})(1 - aq^{1-s} + q^{3-2s})},$$

where a is the trace of Frobenius on the l-adic Tate module of E.

We have identified $H^1(X, \mathbb{Q}_l) = V_l J^\vee$, and $H^1(E, \mathbb{Q}_l) = V_l E^\vee$, cf. [36], Cor. 9.6, and

$$V_l E^\vee \otimes V_l J^\vee \cong \mathrm{Hom}(V_l J, V_l(E))(-1).$$

Hence the rank of $E(k)$, which is equal to the rank of the free quotient $L = \mathrm{Hom}_{\mathbf{F}_q}(J, E)$, is also equal to the multiplicity of q as an eigenvalue of Frobenius on $V_l J^\vee \otimes V_l E^\vee$, by Tate's theorem for abelian varieties over finite fields (Equation (5)). Comparison with the above equation for $L(E/k, s)$ gives

$$\mathrm{ord}_{s=1} L(E/k, s) = \mathrm{rank}\, E(k),$$

and by Theorem 27 the full Birch and Swinnerton-Dyer conjecture is true for the curve E.

Let us write $V_l E^\vee \otimes V_l J^\vee = U \oplus V$, where U is the q-eigenspace of Frobenius, and V is the sum of the other eigenspaces. Then the leading term of the L-series at $s = 1$ is given by

$$\frac{(\log q)^n \det(1 - \mathrm{Frob}\, q^{-1} | V)}{\#E(k)^2_{\mathrm{tors}} q^{-1}} = \frac{1}{q^{g-1}} \frac{\det(L)(\log q)^n}{\#E(k)^2_{\mathrm{tors}}} \#Ш(k, E),$$

where we have applied the conjecture of Birch and Swinnerton-Dyer, and the evaluation of the period $P(E/k) = 1/q^{g-1}$ and the regulator $R(E/k) = \det(L) \cdot (\log q)^n / \#E(k)^2_{tors}$ to obtain the equality with the right hand side. Canceling some terms gives the final identity

$$q^g \det(1 - \mathrm{Frob}\, q^{-1} | V) = \det(L) \#Ш(k, E).$$

The simplest situation is when $V = 0$, so the characteristic polynomial of Frobenius on $V_l E^\vee \otimes V_l J^\vee$ is $(t - q)^{4g}$. We are going to investigate a special case where this happens.

Example. Suppose that q is a square, and write $q = q_0^2$. We choose E so that both eigenvalues of the (arithmetic $\mathbb{F}_q$-)Frobenius are equal to $-q_0$; this can be done, for example, by taking E to be a supersingular curve over $\mathbb{F}_q$ with $q_0 + 1$ points; then recall Equation (4). The existence of such curves E in general is a consequence of Honda-Tate theory [51]; they are obtained as the reduction of elliptic curves with complex multiplication over number fields.

Let X be the non-singular, geometrically irreducible, curve cut out by the Fermat equation

$$x^{q_0+1} + y^{q_0+1} + z^{q_0+1} = 0$$

in $\mathbb{P}^2$. This curve has genus $g = q_0(q_0 - 1)/2$. A simple point count shows that $\#X(\mathbb{F}_q) = q_0^3 + 1$. On the other hand, the Lefschetz fixed

point theorem in étale cohomology gives the number of points as

$$\sum_{i=0}^{2}(-1)^i \operatorname{Tr}(\operatorname{Frob}|H^i(X \otimes \overline{\mathbb{F}}_q, \mathbb{Q}_l)) = q + 1 - \operatorname{Tr}(\operatorname{Frob}|H^1(J, \mathbb{Q}_l)).$$

This can be equal to q_0^3+1 if and only if all the eigenvalues of Frobenius are equal to $-q_0$, since the eigenvalues have absolute value q_0 under any embedding $\overline{\mathbb{Q}}_l \hookrightarrow \mathbb{C}$ [37].

We therefore have $V = 0$, and $L = \operatorname{Hom}_{\mathbb{F}_q}(J, E)$ is a lattice of rank $4g = 2q_0(q_0-1)$. The Birch and Swinnerton-Dyer conjecture then gives

$$\det L \cdot \#Ш(k, E) = q^g = q_0^{q_0(q_0-1)}.$$

Write $q_0 = p^f$. I [23] showed that $Ш(k, E)$ is trivial if and only if $f \leq 2$, while Dummigan [16] has studied the order of $Ш(k, E)$ in the case that $f > 2$. This allows one to compute the determinant of the Mordell-Weil lattice, and in some cases identify its isomorphism type. Here is a table for some small values of q_0; note that $f \leq 2$ in these cases.

q_0	2	3	4
$\operatorname{rank} L$	4	12	24
$\det L$	2^2	3^6	4^{12}
L	D_4	CT_{12}	$2\Lambda_{24}$

Here we obtain the D_4 root lattice, the Coxeter-Todd lattice of rank 12 and a multiple of the Leech lattice of rank 24. A point count can be used to bound the degree of maps $X \to E$, and to show that there are no vectors of norm 2 once $q_0 > 2$. Since the Coxeter-Todd lattice is the unique 12-dimensional even integral lattice of determinant 3^6 with no roots, this identifies L when $q_0 = 3$.

Non-constant curves. We briefly describe which cases of the Birch and Swinnerton-Dyer conjecture are known for general elliptic curves over function fields. Continuing with the notation of the first section, we let E/k be an elliptic curve, and $\pi : S \to X$ the minimal regular model of E. We have an isomorphism $(\pi_* \omega_{S/X})^{\otimes 12} \cong \mathcal{O}_X(\mathcal{D}(E/k))$, where $\mathcal{D}(E/k)$ is the minimal discriminant of E/k. One can show that $\deg \mathcal{D}(E/k)/12 = -(\mathcal{O}_E, \mathcal{O}_E)$, which can take on any non-negative value. E is a constant curve if and only if $(\mathcal{O}_E, \mathcal{O}_E) = 0$.

In the case that $X = \mathbb{P}^1$, the low values of $\deg \mathcal{D}(E/k)$ give (via the classification of surfaces):

$$\begin{aligned} \deg \mathcal{D}(E/k) = 0 &\quad S = E \times \mathbb{P}^1 \text{ is a ruled surface;} \\ = 12 &\quad S \text{ is a rational surface;} \\ = 24 &\quad S \text{ is a K3 surface.} \end{aligned}$$

The conjecture of Birch and Swinnerton-Dyer is known in these cases. The case of rational surfaces is due to Milne [34]. The case of a K3 surface is due to Artin and Swinnerton-Dyer [1]. However, little is known for genuine elliptic surfaces or for surfaces of general type, where the conjecture of Artin and Tate remains open.

There is an analogue of modular curves and Heegner points in the function field setting, beginning with the notions of Drinfeld modules and Drinfeld modular curves. Using this analogy, one can show that the conjecture of Birch and Swinnerton-Dyer is true when the order of the L-function of E/k at $s = 1$ is ≤ 1 [5], [54].

REFERENCES

[1] M. Artin and H. P. F. Swinnerton-Dyer. The Shafarevich-Tate conjecture for pencils of elliptic curves on $K3$ surfaces. *Invent. Math.*, 20:249–266, 1973.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[3] S. Bloch. A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture. *Invent. Math.*, 58(1):65–76, 1980.

[4] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[5] M. L. Brown. *Heegner modules and elliptic curves*, volume 1849 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2004.

[6] Joe P. Buhler, Benedict H. Gross, and Don B. Zagier. On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. *Math. Comp.*, 44(170):473–481, 1985.

[7] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[8] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[9] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[10] T. Chinburg. Minimal models for curves over Dedekind rings. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 309–326. Springer, New York, 1986.

[11] P. Deligne. *Cohomologie étale*. Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier.

[12] Pierre Deligne. Travaux de Shimura. In *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, pages 123–165. Lecture Notes in Math., Vol. 244. Springer, Berlin, 1971.

[13] Pierre Deligne. Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 247–289. Amer. Math. Soc., Providence, R.I., 1979.

[14] Pierre Deligne. Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings). *Astérisque*, (121-122):25–41, 1985. Seminar Bourbaki, Vol. 1983/84.

[15] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[16] Neil Dummigan. The determinants of certain Mordell-Weil lattices. *Amer. J. Math.*, 117(6):1409–1429, 1995.

[17] Noam D. Elkies. Mordell-Weil lattices in characteristic 2. I. Construction and first properties. *Internat. Math. Res. Notices*, (8):343 ff., approx. 18 pp. (electronic), 1994.

[18] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[19] A. Fröhlich. *Formal groups*. Lecture Notes in Mathematics, No. 74. Springer-Verlag, Berlin, 1968.

[20] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[21] Dorian M. Goldfeld. The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 3(4):624–663, 1976.

[22] Benedict H. Gross. Local heights on curves. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 327–339. Springer, New York, 1986.

[23] Benedict H. Gross. Group representations and lattices. *J. Amer. Math. Soc.*, 3(4):929–960, 1990.

[24] Benedict H. Gross. L-functions at the central critical point. In *Motives*, Proc. Sympos. Pure Math., Volume 55, Part 1, pages 527–535. Amer. Math. Soc., Providence, R.I., 1991.

[25] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[26] Alexander Grothendieck. Formule de Lefschetz et rationalité des fonctions L. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55. Soc. Math. France, Paris.

[27] Alexandre Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie - 1960-61 - Revêtements étales et groupe fondamental - (SGA 1)*. Lecture Notes in Mathematics, No. 224. Springer-Verlag, Berlin, New York, 1971.

[28] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[29] Nicholas M. Katz. L-functions and monodromy: four lectures on Weil II. *Adv. Math.*, 160(1):81–132, 2001.

[30] Nicholas M. Katz. *Twisted L-functions and monodromy*, volume 150 of *Annals of Math Studies*. Princeton University Press, New Jersey, 2002.

[31] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[32] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.

[33] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[34] J. S. Milne. The Brauer group of a rational surface. *Invent. Math.*, 11:304–307, 1970.

[35] J. S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.

[36] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[37] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[38] J.S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006.

[39] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[40] A. Néron. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math. (2)*, 82:249–331, 1965.

[41] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967.

[42] Michel Raynaud. Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 286, 129–147. Soc. Math. France, Paris, 1995.

[43] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[44] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[45] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[46] Tetsuji Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990.

[47] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[48] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[49] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[50] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[51] John Tate. Classes d'isogénie des variétés abeliénnes sur un corps fini. In *Séminaire Bourbaki, Vol. 1968/69, Exp. No. 347 - 363*, pages 95–110. Lecture Notes in Math., Vol. 179. Springer-Verlag, Berlin, 1971.

[52] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440, Exp. No. 306. Soc. Math. France, Paris, 1995.

[53] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[54] Douglas Ulmer. Elliptic curves and analogies between number fields and function fields. In *Heegner points and Rankin L-series*, volume 49, pages 285–315. MSRI Publications, Berkeley, 2004.

[55] André Weil. *Adeles and algebraic groups*, volume 23 of *Progress in Mathematics*. Birkhäuser Boston, Mass., 1982. With appendices by M. Demazure and Takashi Ono.

[56] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[57] Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.

[58] Shouwu Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math. (2)*, 153(1):27–147, 2001.