ELLIPTIC CURVES AND MODULAR FORMS

Contents

Date: Spring 2010.

These notes are taken from a course on elliptic curves and modular forms taught by Jordan Ellenberg at the University of Wisconsin in Spring of 2010.

The main reference for the course (and these notes) are Silverman's book AEC (for elliptic curves) and Diamond and Shurman's book FCMF (for modular forms.)

1. January 21, 2010

Let k be a field. The *k rational points of projective n-space* $\mathbb{P}^n(k)$ which consists of

$$\{(x_0 : x_1 : \cdots : x_n) \mid x_i \in k \text{ not all zero}\}/\sim$$

with the equivalence relation $(x_0 : \cdots : x_n) \sim (y_0 : \cdots : y_n)$ if there exists $c \in k$ such that $x_i = cy_i$ for all $i = 0, \ldots, n$.

$\mathbb{P}^n(k)$ is almost in bijection with k^n:

$$\mathbb{P}^n(k)\backslash \longrightarrow k^n \qquad (x_0 : \cdots : x_n) \mapsto \left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$$

is a bijection with inverse $(y_1, \ldots, y_n) \mapsto (1 : y_1 : \cdots : y_n)$.

By a *plane curve of degree d* we mean a polynomial $f \in k[X, Y, Z]$ which is *homogeneous* of degree d, i.e. each monomial is of degree d. e.g. $f(X, Y, Z) =$

$X^2 + Y^2 - Z^2$ is a plane curve of degree 2. The vanishing locus of f is often denoted

$$V(f) = \{x \in \mathbb{P}^2(x) \mid f(x) = 0\} \subset \mathbb{P}^2.$$

Note that

$$f(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, s_n) \tag{1.0.1}$$

so the vanishing set is well defined.

Exercise 1.0.1. If k is algebraically closed show that (1.0.1) holds if and only if f is homogeneous of degree d.

How do we draw the plane curve $f = X^2 + Y^2 - Z^2$ for which we often write $V(f) = C$? The easiest way is to draw the piece of $V(f)$ that sits in affine space. For example, look at the set of $(1 : y : z)$ such that $f(1, y, z) = 1 + y^2 - z^2 = 0$. If $k = \mathbb{R}$ this is a hyperbola (picture drawn in class.) However, it is missing the points when $X = 0$, i.e. solutions to $f(0, Y, Z)$:

$$V(f) \cap \{X = 0\} = \{(0 : Y : Z) \mid y^2 = z^2\} = \{(0 : 1 : 1), (0 : 1 : -1)\}.$$

These are the *points at infinity.*

Alternatively, we could look at a different chart ($\{Z \neq 0\}$.) Then we get $x^2+y^2 = 1$ which is a circle. Is this the whole curve? Yes, as one can see by noting that

$$C(\mathbb{R}) = C(\mathbb{R}) \cap \{Z \neq 0\} \cup C(\mathbb{R}) \cap \{Z = 0\}.$$

The latter set is easily seen to be empty.

If $k = \mathbb{F}_q$, $C(k)$ is a finite set. It is natural to study $\#C(k)$. If $k = \mathbb{R}$, $C(k)$ is a 1-dimensional space. If $k = \mathbb{C}$, $C(k)$ is a 2-dimensional real space, i.e. a surface. (For example, for our $f = X^2 + Y^2 - Z^2$, $C(\mathbb{C})$ is a sphere.)

1.1. **Why define a curve to be f rather than $V(f) \subset \mathbb{P}^2(k)$?** One reason: let

$$f = X^2 + Y^2 - Z^2, \quad g = (X^2 + Y^2 - Z^2)^2$$

for which $V(f) = V(g)$. If we let these be the same we would run into problems. For example, one could consider the family of curves $(X^2 + Y^2 - Z^2)^2 - tX^2Y^2$ for varying t. We would like this to have the same degree for all t, but this wouldn't be the case if f and g were the same. (The curve g is called *non-reduced*, and is thought of as a "double copy" of f.)

1.2. **Cubic plane curves.** A *cubic plane curve* over k is

$$C : F = c_1X^3 + c_2Y^3 + c_3Z^3 + \cdots + c_{10}XYZ$$

up to multiplication by $k^\times$.

The key fact (that we will prove) is that $C(k)$ can often be given the structure of an abelian group which will satisfy the following. Let ℓ be a line in $\mathbb{P}^2(k)$, i.e. a linear polynomial $aX + bY + cZ$. Consider $\ell \cap C$ which consists of $P \in C(k)$ such that $\ell(P) = 0$. This is to say (assuming $c \neq 0$, which we may do without loss of generality) that $Z = -\frac{1}{c}(aX + bY)$. Substitute this into $F(X, Y, -\frac{1}{c}(aX + bY)) = G(X, Y)$. Then we ask how many solutions there are. For example, $G(X, Y)$ could be $X(X-Y)(X+Y)$ which has the three solutions $(0 : 1 : \underline{/}c), (1 : 1 : -(a+b)/c), (1 : -1 : (b - a)/c)$. In general, there will be at most three solutions corresponding to the roots of $G(X, Y)$ unless $G = 0$. (An example of $G = 0$: $C : X(X^2 + Y^2 + Z^2)$ and $\ell : X$.)

The group law on $C(k)$ (when C is smooth) will satisfy the property

(1.2.1) If ℓ is a line and $C \cap \ell = \{P, Q, R\}$ then $P + Q + R = 0$.

What is smoothness? One characterization is that if C is smooth then given $P, Q \in C(k)$ there exists a unique $R \in C(k)$ such that there exists $\ell\mathbb{P}^2(k)$ with $\ell \cap C = \{P, Q, R\}$. Given this, the natural first try for ℓ would be the line in $\mathbb{P}^2(k)$ going through P and Q. This is well defined so long as $P \neq Q$, in which case $\ell \cap C$ is in bijection with the roots of $G(X, Y)$. Since P, and Q correspond to two rational roots, the third must be rational as well.

If $P = Q$ we would want ℓ to be the tangent line to C at P (which is well defined if C is smooth.) In this case G will have a double root corresponding to P and R will correspond to the third root.

2. January 26, 2010

2.1. **A little bit about smoothness.** Recall from calculus that if $C = V(f)$, $f \in k[X, Y, Z]$ is homogeneous of degree d then we say f is *smooth* at P if it's not the case that $f, \frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y, \frac{\partial f}{\partial X}}, \frac{\partial f}{\partial Z}$ all vanish at P. We say C is smooth if it's smooth at every *geometric point*, i.e. for every $P \in C(\overline{k})$.

An example: $f = X^3 + Y^3 + Z^3$. Then

$$\frac{\partial f}{\partial X} = 3X^2, \quad \frac{\partial f}{\partial Y} = 3Y^2, \quad \frac{\partial f}{\partial Z} = 3Z^2.$$

So to be smooth need $X = Y = Z = 0$ which is not a point of $\mathbb{P}^2$. UNLESS $char k = 3$ in which every point is singular, i.e. not smooth. (Note that in this case $f = (X + Y + Z)^3$, so C is a triple line.)

Now let's assume $3 \neq 0$. To find the tangent line at $P = (1 : 0 : -1) \in C$ we consider the line

$$\left.\frac{\partial f}{\partial X}\right|_P X + \left.\frac{\partial f}{\partial Y}\right|_P Y + \left.\frac{\partial f}{\partial Z}\right|_P Z.$$

So we get $L_P : X + Z$. The intersection $L_P \cap C$ must satisfy $X = -Z$ which implies that $Y^3 = 0$. We conclude that the third point of intersection is also P. We write $L_P \cap C = 3P$. Our group law must satisfy $P + P + P = 0$.

A smooth point P on a curve C (of degree greater than one) where the tangent line to P intersects P more than twice is called a *flex point.* If P is flex then we must have that $P + P + P = 0$. (We will see that the converse is also true.)

Flex points (at least when the characteristic is bigger than three) a characterized by those points for which the Hessian

$$\det \begin{pmatrix} \frac{\partial^2 f}{\partial X^2} & \frac{\partial^2 f}{\partial X \partial Y} \\ \frac{\partial^2 f}{\partial X \partial Y} & \frac{\partial^2 f}{\partial Y^2} \end{pmatrix}$$

vanishes. (Given that this is different than f) there should be 9 flex points.

We can also see the tangent line by studying the Taylor expansion of f in affine coordinates which vanish at P. Examples of affine coordinates are $x = \frac{X}{Z} + 1 = \frac{X+Z}{Z}, y = \frac{Y}{Z}$. (In general, affine coordinates are ratios of linear homogeneous polynomials.) In this coordinate system we rewrite the curve as

$$x^3 - 3x^2 + 3x + y^3 = (x - 1)^3 + y^3 + 1.$$

This has Taylor expansion $3x + h.o.t.$ (higher order terms) from which we see that the tangent line is given by $3x = 0 \implies X + Z = 0$.

A singular example: $f = Y^2Z + X^3 + X^2Z$. Check that $(0:0:1)$ is non-smooth:

$$\frac{\partial f}{\partial X} = 3X^2 + 2XZ, \quad \frac{\partial f}{\partial Y} = 2YZ, \quad \frac{\partial f}{\partial} = Y^2 + Z^2.$$

Set $x = X/Z, y = Y/Z$ to get

$$f(x,y) = y^2 + x^2 + x^3 = x^2 + y^2 + h.o.t. = (x - iy)(x + iy) + h.o.t.$$

We see that there is no tangent line (i.e. linear term) but near the origin it look like the union of two lines. (Picture drawn in class of what this curve looks like over $\mathbb{R}$ which has an isolated point at the origin.)

Exercise 2.1.1. Find all singular points of $Y^2Z + X^3 + X^2Z$. (Note that this may be dependant upon the characteristic of k.)

Exercise 2.1.2. Give an example of a set S and two different group laws $+_1, +_2$ such that

$$\{(P,Q,R) \mid P +_1 Q +_1 R = 0\} = \{(P,Q,R) \mid P +_2 Q +_2 R = 0\}.$$

Question/Hint: What is the identity in $C(k)$? Suppose that O is the purported identity. Then $O + O = O = -O \implies O + O + O = 0$, and so O is a flex point.

Theorem 2.1.3. *Suppose that C/k is a smooth cubic plane curve and $O \in C(k)$ is a flex point. Then there is a unique group law on $C(k)$ such that $P + Q + R = 0$ whenever $\{P,Q,R\} = L \cap C$ and O is the identity.*

An example of a curve with no flex points. Can check that $3X^3 + 4Y^3 + 5Z^3$ has no flex points i and only if one of $3/5, 4/5, 4/3$ is a cube in k.

2.2. **Weierstrass form.** What is $P + Q$? Answer: if R is the third point of intersection of the line connecting P and Q. Then $P + Q$ is the third point of intersection on the line connecting R and O.

Given (C, O) as above, let's put O at the point $(0:1:0)$ by applying a projective linear change of coordinates. We may, moreover, make the tangent line to C at O be the line $Z = 0$ because the action of $\mathrm{PGL}_2(k)$ on $\mathbb{P}^k$ is double transitive. Setting $Z = 0$ gives

$$a_1X^3 + a_2X^2Y + a_3XY2 + a_4Y^3.$$

Since $(0:1:0)$ must be a triple zero, this implies that $a_2 = a_3 = a_4 = 0$. After a further (simple) change of variables we see that C can be written in the form

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

or, in affine coordinates $x = X/Z, y = Y/Z$:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2.1}$$

If *chark* $\neq 2$ then eliminate the xy and y terms by completing the square, and if *chark* is zero or greater than 3 it can be further simplified to

$$y^2 = x^3 + Ax + B \qquad \text{or} \qquad y^2 = x^3 - 27c_4x - 54c_6.$$

Is C smooth? Let us work with $F : y^2 = x^3 + Ax + B = f(x)$. Then

$$\frac{\partial F}{\partial x} = -(3x^2 + A) = -f'(x), \quad \frac{\partial F}{\partial y} = 2y.$$

So a non-smooth point must satisfy $y = f(x) = f'(x) = 0$ which is equivalent to the discriminant of f $\Delta = -16(4A^3 + 27B^2) = 0$.

3. January 28, 2010

Equation (2.2.1) is a smooth cubic plane curve with flex point over k if $a_1, a_2, a_3, a_4, a_6 \in k$ and $\Delta \neq 0$. The existence of the group law can now be proved by formula. This is not conceptually satisfying but it works, and it is very messy. In particular, checking associativity is quite a computation.

As an example suppose $E : y^2 = 4x^3 + b_2x^2 + b_4x + b_6$. Then if $P = (x, y)$, the x-coordinate of $2P$ is

$$\frac{x^4 - b_4x^2 - 2b_6 - b_8}{4x^3 + b_2x^2 + b_4x + b_6}.$$

Note that this doesn't depend on y. The reason for this is that on this curve the identity O is the point at infinity in the "straight up" direction. Thus $-(x, y) = (x, -y)$. So if $x(P) = x(Q)$ then $P = \pm Q$, and $x(2Q) = x(2P)$.

Note also that the denominator of $x(P) = 0$ exactly when $y^2 = 0$ which means $y = 0$. This happens if and only if $2P = O$.

3.1. An algebro-geometric description of the group law in terms of divisors.

Let (E, O) be an elliptic curve over k. (Can view this in two different ways. Either this means that E is a genus curve with a point O or a curve in Weierstrass form with $O = (0 : 1 : 0)$.) We will assume now that k is algebraically closed.

A *divisor* on E is a formal finite sum $\sum n_iP_i$ where $n_i \in \mathbb{Z}$ and $P_i \in C(k)$. If $f \in k(C)$ is a rational function define $div f = \sum_{P\in C(k)} \mathrm{ord}_P(f)P$ where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P (hence negative if f has a pole at P.)

Example: $C = \mathbb{P}^1$. Then $k(C) = k[z]$. We have $div\left(\frac{z-1}{z+1}\right) = [-1] - [1]$, $div(z^2 + 1) = [i] + [-i] - 2[\infty]$, ... By the way, in this second case one can see that the answer is as claimed by changing variables to $z = 1/w$. Then $div(1/w^2 + 1) = div\left(\frac{w^2+1}{w^2}\right) = [i] + [-i] - 2[0]$. Then going back to the original coordinates gives the result.

The point of talking about divisors is it gives a good "geometric" way to seeing what's going on.

If $D = \sum n_iP_i$ then *degree of* D is $\deg D = \sum n_i$.

Theorem 3.1.1. *If* $f \in k(C)$ *then* $\deg(div(f)) = 0$.

We say that D is *principal* if $D = div(f)$ for some $f \in k(C)$. Denote $Prin(C)$ for the group of principal divisors, $Div^0(C)$ the group of degree 0 divisors and $Div(C)$ the group of divisors. The *Picard group of* C is $\mathrm{Pic}^0(C) = Div^0(C)/Prin(C)$.

Easy to prove fact: $\mathrm{Pic}^0(\mathbb{P}^1) = 0$.

Note that $div(cf) = div(f)$ for all $c \in k^\times$. In fact,

$$1 \to k^\times \to k(C)^\times \to Prin(C) \to 0$$

is exact.

Given a curve C and a point $O \in C(k)$ we have an Abel-Jacobi map

$$AJ : C(k) \to \mathrm{Pic}^0(C) \qquad P \mapsto [P] - [O]. \tag{3.1.1}$$

Now we restrict to the case of genus one, and we'll prove that AJ is a bijection in this case.

Injectivity: Suppose that $AJ(P) = AJ(Q)$ and $P \neq Q$. This means that $P-O = Q-O \in \mathrm{Pic}^0(C)$, so $P-Q = div(f)$ for some f. We can think of $f : C \to \mathbb{P}^1$. Then $f^{-1}(0) = P$ and $f^{-1}(\infty) = \{Q\}$. This implies that f has degree 1 which happens if and only if f is a bijection. This, however, is a contradiction because $\mathbb{P}^1$ has genus 0.

We say that a divisor $D = \sum n_p P$ is *effective* if $n_p \geq$ for all P, and write this as $D > 0$. Similarly, we can define when $D_1 \geq D_2$. Let $\mathcal{L}(D)$ be the space of functions such that $div f \geq -D$ (which means that $\mathrm{ord}_P(f) \geq -n_P$. We can think of this as "the space that has poles at worst $-D$.") So, for example, $\mathcal{L}(0)$ is the space of holomorphic functions. The Riemann-Roch theorem in genus 1 implies that if D is a divisor of degree $d > 0$ then $\mathcal{L}(D)$ has dimension d.

We use R-R to prove surjectivity. Let $D = P_1 + \cdots P_n - Q_1 - \cdots - Q_n$. So R-R applied to $D + O$ gives a one dimensional space and therefore a unique up to scalar f. We study $div(f)$ which has k zeroes and k poles. The definition of $\mathcal{L}(D)$ implies that $m \leq k \leq m+1$. First, suppose that $k = m$. Then $div(f) + D + O \geq 0$ which implies that

$$div f = -D - O + R \qquad R \in \{P_1, \ldots, P_n, O\}.$$

So $-D - O + R = 0$ in $\mathrm{Pic}^0(C)$ which implies that $D = R - O = AJ(R)$. The proof is nearly identical when $k = m+1$. Again this implies $div f = -D - O + R$, but in this case the only difference is that $R \notin \{P_1, \ldots, P_n, O\}$.

The group law on $\mathrm{Pic}^0(C)$ then transfers to E via the bijection AJ.

Theorem 3.1.2. *Let k be any field. Any elliptic curve (E, O) over k can be embedded in $\mathbb{P}^2$ as a smooth cubic in Weierstrass form.*

Note: The point O can be any point defined over k. Actually the property of being a flex point is particular to a given embedding of C in projective space and not intrinsic to the curve.

3.2. Why are the two group laws the same?

If $P +_E Q +_E R = 0$ should mean that

$$div(f) = (P - O) + (Q - O) + (R - O) = P + Q + R - 3O.$$

Indeed, can take $f = \frac{\ell(X,Y,Z)}{Z}$ where ℓ is the line intersecting the curve at $\{P, Q, R\}$.

4. February 2, 2010

4.1. Overview.

We have now established that when E is an elliptic curve (we drop the notation (E, O) from now on, but implicitly E is a curve *and* a point) and k is a field, $E(k)$ is an abelian group. So we can consider $E/\mathbb{Q}$ as a functor

$$E : \text{Fields} \to \mathbb{Q}\text{-alg}$$

called the *functor of points*. (More generally, it is a functor form rings to abelian groups, but we don't have the language to quite understand this now.)

Of course, a functor must also respect morphisms. That is to say that if $\phi : k \to l$ is a map of fields then there is a map $E(\phi) : E(k) \to E(l)$ which functorial (meaning it respects compositions of morphisms...)

For an algebraic geometer an elliptic curve is not a "complex torus" even though $E(\mathbb{C})$ is a complex torus. Instead, he/she thinks of an elliptic curve in terms of this functor.

We will see that $E(\mathbb{C})$ is a complex torus, and that there are many such objects of different 'shape.' We will also study $E(\mathbb{Q})$ which can be many things. Since $E(\mathbb{F}_q)$ is finite we will be interested in computing its order and structure.

Why do we study degree 3 curves? Well, for one it is the easiest non-trivial case. If C is a degree 2 plane curve then $C(\mathbb{C}) \simeq \mathbb{CP}^1$, a sphere; $C(\mathbb{Q})$ is either empty or easily shown to be in bijection to $\mathbb{P}^1(\mathbb{Q})$ and $C(\mathbb{F}_q)$ has size $q+1$.

4.2. **Uniqueness of Weierstrass form.**

Can the same elliptic curve have different Weierstrass forms? By "same" one can mean "there is a projective linear transformation taking one Weierstrass form to another" or "isomorphic as abstract curves."

The answer is "yes." In fact, any linear transformation that takes one Weierstrass form to another is of the form

$$(x, y) \mapsto (u^2x' + r, u^3y' - u^2xs' + t).$$

If the original Weierstrass form is

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

then after this change of variables, one obtains

$$(y')^2 + a_1'x'y' + a_3'y' = (x')^3 + a_2'(x')^2 + a_4'x' + a_6'$$

where, for example,

$$ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2, \ldots$$

So a_1 is not an invariant of an elliptic curve (unless the characteristic of k is 2...) However, certain functions of the a_i do behave better. For example,

$$c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3)$$

satisfies $u^4c_4' = c_4$. How might one find such a relation? Well, one way is by "invariant theory" as studied by 19th century mathematicians who were very good at manipulating such things (and for whom the relation for c_4 above would not have been too challenging.) A more natural way, however, is to find c_4 by doing the manipulations that we did to get a Weierstrass equation in the form $y^2 = x^3 - 27c_4x - 54c_6$. Similarly, c_6 satisfies $u^6c_6' = c_6$.

One can further define Δ as a polynomial in the a_i's such that

- $\Delta = 0$ if and only if E is non smooth
- $1728\Delta = c_4^3 - c_6^2$, and so $u^12\Delta' = \Delta$.

If the characteristic is not 2 or 3 then this is the same Δ as described above as the discriminant of $x^3 - 27c_4x - 54c_6$.

Now we have a true invariant:

$$j := \frac{c_4^3}{\Delta} = 1728 + \frac{c_6^2}{\Delta}.$$

That is to say that $j(E)$ is independent of the choice of Weierstrass equation.

Two examples. Let

$$E_1 : y^2 = x^3 - x, \qquad E_2 : y^2 = x^3 - 1 \tag{4.2.1}$$

In the first case $c_6 = 0$ so $j(E_1) = 1728$, and in the second case $c_4 = 0 \implies j(E_2) = 0$.

Theorem 4.2.1. *Let k be an algebraically closed field. Let E_1, E_2 be elliptic curves over k. Then $E_1 \simeq E_2$ if and only if $j(E_1) = j(E_2)$.*

Proof. We have seen directly that isomorphic elliptic curves have the same j-invariant. To show that the converse is true we prove that if $j(E_1) = j(E_2)$ then the two curves are isomorphic. For simplicity, we take characteristic not equal to 2 or 3. Write

$$E_i : y^2 = x^3 + A_i x + B_i$$

for $i = 1, 2$. Then we know, that

$$\frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27B_2^2}$$

from which is follows that

$$\frac{27B_1^2}{4A_1^3} = \frac{27B_2^2}{4A_2^3}.$$

Thus, we can write $(A_2, B_2) = (u^4 A_1, u^6 B_1)$ for some $u \in k$. We have seen already that the change of coordinates $(x, y) \mapsto (u^2 x, u^3 y)$ changes $E_1 \to E_2$ so they are isomorphic. □

Note that we are use the fact that k is algebraically closed to get the element u. As an example, notice that the curves

$$y^2 = x^3 + x + 1 \qquad \text{and} \qquad y^2 + x^3 + 4x + 8$$

are isomorphic over $\overline{\mathbb{Q}}$ (in fact, they are isomorphic over $\mathbb{Q}(\sqrt{2})$.) They are not isomorphic over $\mathbb{Q}$.

More is true.

Theorem 4.2.2. *Let k be any field. For any $j_0 \in \overline{k}$ there exists an elliptic curve defined over $k(j_0)$ having j-invariant j_0. Thus the j-invariant gives a bijection between the set of isomorphism classes of elliptic curves over $\overline{k}$ and elements of $\overline{k}$.*

Proof. All we need to show is that the j-invariant is surjective. To do this, let $k = \mathbb{Q}(t)$ and write down an elliptic curve E^{univ}/k with $j(E) = t$:

$$y^2 + xy = x^3 - \frac{3t}{t + 1728} x - \frac{1}{t - 1728}$$

If $j_0 \neq 0$ or 1728 then this curve specializes to a curve over $\overline{k}$ by substituting $t = j_0$. To prove the remaining two cases, we observe that the curves from (4.2.1) so long as the characteristic is not 2 or 3. The remaining cases can be handled individually. □

5. February 4, 2010

5.1. **The invariant differential.** Given an elliptic curve in Weierstrass form (2.2.1), we define the *invariant differential* to be

$$\omega = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}.$$

If $a_1 = a_2 = a_3 = 0$ then $\omega = \frac{dx}{2y} = \frac{dy}{3x^2 + a_4}$.

What is dx? More generally, what is a differential form? The answer can be given purely algebraically.

In algebraic geometry a *function* on E (or rather on the affine part $E - 0$) is an element of the *coordinate ring* $R = k[x, y]/(y^2 + \cdots = x^3 + \cdots)$. These can be thought of as the 0-forms.

Hartshorne II.8 gives definitions of differentials: If R is a k-algebra, the space of 1-forms on R over k is the free R-module generated by df for all $f \in R$, with the equivalence relations

- $d(fg) = gdf + fdg$ for all $f, g \in R$,
- $da = 0$ for all $a \in k$,
- $d(f+g) = df + dg$ for all $f, g \in R$.

One can check that this is k-linear: $d(af) = adf + fda = adf$. It behaves (as is proved in Hartshorne) the way you would expect.

Some remarks. We can define a differential on all of E (not just the affine part) whose restriction is ω. Up to scaling, ω is the only differential form on E. Note that $(1 + x + y^2)\omega$ is also a differential form on $E - 0$, but it doesn't extend to all of E because it blows up at infinity.

It is a fact that if X is a smooth projective curve over k then the 1-forms on X over k form a finite dimensional k vector space. This dimension is called the *genus* of the curve.

Let us examine the example of $\mathbb{P}^1$ and the differential dz. The question is rather or not this is defined at ∞. To see this make the change of coordinates $w = 1/z$. Then $dz = -\frac{1}{w^2}dw$ (as expected) and thus a double pole at infinity. We can write $divdz = -2[\infty]$.

If ω is a 1-form on X, $div(\omega)$ is called a *canonical divisor* on X. It is a fact that if ω' is another 1-form then $\omega' = f\omega$ for some $f \in k(X)$. Therefore, $div(\omega') = div(\omega)$ in $\mathrm{Pic}(X)$. As an element of $\mathrm{Pic}(X)$ is called the *canonical class* and is denoted K_X. It has degree $2g - 2$.

One can check that ω (as defined at the beginning of this section) is holomorphic on all of E and that $div(\omega) = 0$, implying that $K_E = 0$. For this reason ω is sometimes called the *holomorphic differential* or the *trivial differential.*

We now explain why ω is called 'invariant.' If $P \in E(k)$ we have a map

$$t_P : E \to E \qquad Q \mapsto P + Q.$$

This induces a map on differential forms. For example, if $\phi : E \to k$ is a 0-form then $(t_P^*\phi) = \phi(t_p(Q)) = \phi(P + Q)$. In algebro-geometric language, the map on 1-forms is

$$t_P^* : \Gamma(E, \Omega^1_{E/k}) \to \Gamma(E, \Omega^1_{E/k})$$

where $\Gamma(E, \Omega^1_{E/k})$ is the space of "global sections of 1-forms."

Thus $f_P^*\omega$ is a holomorphic differential on E which can't be zero because the map ${}^*_P$ is invertible. (It's inverse is t^*_{-P}.) In other words, t_p^* is an element of $k^\times$, i.e. a map $E(k) \to k^\times$. In fact, this is an algebraic map $E \to \mathbb{G}_m = \mathbb{A}^1 - 0$ of varieties. From algebraic geometry, we know that a map from a projective variety X to an affine variety A must be constant. Putting this together with the fact that t_0^* acts by 1 on differentials, it follows that $t_P^*\omega = \omega$ for all P.

If is a fact that under the usual change of coordinates $(x, y) \mapsto (u^2x', u^3y')$ we get that $u^{-1}\omega' = \omega$. As we have discussed the map

$$\{\text{Weierstrass forms}\} \longrightarrow (E, O)$$

is surjective but not injective. However, we now have that

$$\{\text{Reduced Weierstrass forms} longrightarrow (E, O, \omega)$$

is one-to-one. (By "reduced" we mean in the form $y^2 = x^3 + Ax + B$.)

5.2. **First glimpse of modular forms and modular functions.** A description (not a definition): a *modular function* is an algebraic function F on equivalence classes of elliptic curves. For example, the j-invariant. A *modular form* is an algebraic function F on equivalence classes of pairs (E, ω) such that

- $F(E, \lambda\omega) = \lambda^{-k} F(E, \omega)$ for some $k \in \mathbb{Z}$ (called the weight) and all $\lambda \in k$, and
- F has "slow growth at infinity."

Examples of these are c_4 and c_6 which are modular forms of weights 4 and 6 respectively.

Why is c_4 a modular form? The "function"

$$F(y^2 = x^3 - 27c_4x - 54c_6) = c_4$$

is not well defined on E because there are several Weierstrass forms for the same elliptic curve. However, having fixed ω a change in Weierstrass form would also change ω. Concretely, if we scale x by u^2 and y by u^3 then ω will be changed by a factor of u^{-1} and c_4 by u^4.

Comment: If the characteristic of k is 2, then a_1 is a modular form of weight 1.

6. February 9, 2010

6.1. **Isogenies.** Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism of curves $\phi : E_1 \to E_2$ such that $\phi(O_{E_1}) = O_{E_2}$. An example is the multiplication by m map

$$[m] : E \to E \qquad [m]P = \operatorname{sgn} m(\underbrace{P + P + \cdots + P}_{|m| \text{ times}}).$$

Note that the multiplication by 2 map is the composition of

$$\begin{tikzcd} E \arrow[r, "\Delta"] & E \times E \arrow[r, "m"] & E \end{tikzcd}$$

where Δ is the diagonal embedding and m is the group action $m(P, Q) = P + Q$.

Another example of a morphism can be given between the curves

$$E : y^2 = x^3 + ax^2 + bx \qquad E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x. \tag{6.1.1}$$

One can check that $\phi(x, y) = \left(\frac{y^2}{x^2}, y\frac{b-x^2}{x^2}\right)$ is an isogeny from E to E'.

Let us discuss how one can see that $O_E \mapsto O_{E'}$ in an informal way. As we move towards ∞ on either of the curve $x \sim t^2$ and $y \sim t^3$. So the x-coordinate of $\phi(x, y)$ grows like $\frac{(t^3)^2}{(t^2)^2} = t^2$, and the y-coordinate grows like $t^3\left(\frac{1}{t^2} - 1\right) \sim t^3$. So, by continuity the origin of E must go towards that of E'.

Note that if we try to projectivize the equation for ϕ, we would get

$$\phi(X : Y : Z) = (Y^2Z : bYZ^2 - X^2Y : X^2Z) \tag{6.1.2}$$

which is not defined at $(0 : 1 : 0)$ (or at $(0 : 0 : 1)$.) In fact, only linear maps from $\mathbb{P}^2$ to $\mathbb{P}^2$ are defined everywhere. Higher degree "maps" (it's not a morphism but rather a *rational* map denoted $V \dashrightarrow V'$) between projective varieties V and V', may not be defined on a subvariety of at most codimension 2 in V. Even though ϕ does not extend to a morphism on all of $\mathbb{P}^2$ its restriction to E can (must if we believe it's a morphism!) be defined. Actually, the codimension 2 fact above, implies that it must be defined on all of E.

Exercise 6.1.1 (OPTIONAL). Show that ϕ can be defined on all of E using an equivalent definition of ϕ near the points at which (6.1.2) is not defined.

Solution. The map ϕ is given by the following in projective coordinates.

$$\begin{aligned}\Phi(X:Y:Z) =&(Y^2Z : bYZ^2 - X^2Y : X^2Z)\\ &= (XY^2 : bXYZ - \frac{X^3Y}{Z} : X^3)\\ &= (XY^2 : bXYZ - (Y^2 - aX^2 - bXZ)Y : X^3) \qquad ((X:Y:Z) \in E)\\ &= (XY^2 : 2bXYZ - Y^3 + aX^2Y : X^3)\end{aligned}$$

Now, using this manifestation of ϕ, it is clear that $\phi(0:1:0) = (0:1:0)$. □

Following the same line of reasoning as above to determine $\phi(O_E) + O_{E'}$ we will analyze what $\phi(0,0)$ is. If $x \sim t$ then, since $y^2 = bx + \cdots$, $y \sim t^{1/2}$. Then

$$\phi(x,y) \sim \left(\frac{bx}{x^2}, \frac{b^{3/2}}{x^{3/2}}\right) \sim (t^{-1}, t^{-3/2}).$$

Taking $s = t^{-2}$ (which is growing we see that the x-coordinate of $\phi(x,y)$ grows like s^2 and the y-coordinate grows like s^3, hence $\phi(0,0)$ must be $O_{E'}$.

When ϕ is a nonzero isogeny, the *degree of* ϕ is the degree of the field extension $k(E_1)/k(E_2)$. Note that rational functions on E_2 pull back to functions on E_1 via the map ϕ. The degree of the zero map is taken to be zero.

It's a fact that if $f : C_1 \to C_2$ is a map of curves over an algebraically closed field k of characteristic zero then $\deg f = \#f^{-1}(P)$ for all but finitely many $P \in C_2(k)$. In the case of isogenies between elliptic curves we can remove the restriction "all but finitely many points."

As an example, consider the map $\mathbb{P}^1 \to \mathbb{P}^1$ given by $z \mapsto z^2$. For every $w \in \mathbb{P}^1(\mathbb{C})$ except $w = 0$ or ∞, there are two points in the preimage of w. Evidently, this map has degree two. This is verified by noting that the inclusion of function fields under this map is $k(z^2) \subset k(z)$ which clear is degree two.

Question: If E_1, E_2, ϕ are all defined over $\mathbb{Q}$ is $\deg(\phi_K)$ the same for any $K/\mathbb{Q}$. The answer is yes.

Exercise 6.1.2. Show that the isogeny ϕ between the curves (6.1.1) has degree 2.

Exercise 6.1.3. Let $k = \mathbb{C}$. Describe all choices of a, b such that $E \simeq E'$ (i.e. $j(E) = J(E')$.) In the case these cases there exists $i : E' \to E$. Show that $i \circ \phi : E \to E$ is not $[m]$ for any $m \in \mathbb{Z}$.

Let $k = \mathbb{F}_q$ where $q = p^m$ and p is prime. Let E/k be an elliptic curve. (e.g. $E : y^2 = x^3 + Ax + B$) The map $Fr : (x,y) \mapsto (x^q, y^q)$ is an isogeny from E to E.

Fact (to be proven later): The degree of Fr is q. However, if $P = (x,y) \in E(\overline{\mathbb{F}}_q)$ its preimage consists of the single point $(x^{1/q}, y^{1/q})$ because $Fr : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ is a bijection.

Additional facts:

- If ϕ_1, ϕ_2 are isogenies over k then so is $\phi_1 + \phi_2$. So $\mathrm{Hom}_k(E_1, E_2)$ is an abelian group.
- $\mathrm{Hom}_k(E,E) = \mathrm{End}_k(E)$ is a ring with multiplication given by composition of isogenies.

- $\deg : \mathrm{End}_k(E) \to \mathbb{Z}$ respects multiplication: $\deg(\phi_1\phi_2) = \deg(\phi_1)\deg(\phi_2)$. Since $\deg(\phi) = 0$ if and only if $\phi = 0$ this implies that $\mathrm{End}_k(E)$ has no zero divisors.
- Every isogeny $\phi : E_1 \to E_2$ is also a group homomorphism.

To see why the last item is true consider the diagram

$$\begin{tikzcd}
E_1 \arrow[r, "AJ_1"] \arrow[d, "\phi"'] & \mathrm{Pic}^0(E_1) \arrow[r, hook] & Pic(E_1) \arrow[d, dashed, "\phi_*"] \\
E_2 \arrow[r, "AJ_2"] & \mathrm{Pic}^0(E_2) \arrow[r, hook] & Pic(E_2)
\end{tikzcd}$$

The map $\phi_* : \mathrm{Pic}(E_1) \to \mathrm{Pic}(E_2)$ is defined on the level of divisors to be the group homomorphism sending P to $\phi(P)$. Have to check that this gives a well defined map $\mathrm{Pic}(E_1) \to \mathrm{Pic}(E_2)$. In other words, need to see that it sends principal divisors to principal divisors. Let $f \in k(E_1)$. Then one can check that $\phi_*(div(f)) = div(N_{k(E_1)/k(E_2)}f)$.[1] Proof of this is left to the student.

Since Pic^0 is a subgroup of Pic this gives a map (also denoted ϕ_*) from $\mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ that is, by definition, a group homomorphism. To complete the proof, we must show that the diagram commutes. Suppose $P \in E_1(k)$. Then $AJ_2 \circ \phi(P) = \phi(P) + O_{E_2}$, and $\phi_* \circ AJ_1(P) = \phi_*(P + O_{E_1}) = \phi(P) + \phi(O_{E_1}) = \phi(P) + O_{E_2}$, so indeed it does commute.

7. February 11, 2010

Last time we saw that if $\phi : E_1 \to E_2$ is an isogeny[2], then $\ker\phi$ is a finite subgroup of E_1.

7.1. Galois theory of isogenies.

Let $\phi : E_1 \to E_2$ be an isogeny over an algebraically closed field k. The following is true.

- For any $Q \in E_2(k)$, $\#\phi^{-1}(Q) = \deg_s \phi$ where $\deg_s$ is the *separable* degree. (e.g. $\deg_s(Fr) = 1$.)
- The *inseparable degree* $\deg_i \phi = e_\phi(P)$ for each $P \in E_1(k)$.
- When ϕ is separable (i.e. $deg_s\phi = \deg\phi$) then $k(E_1)/k(E_2)$ is a Galois extension with Galois group $\ker\phi$.

To prove the final point, have to show that $\ker\phi$ acts on $k(E_1)$ preserving $k(E_2)$. Let $P \in \ker\phi$. Then the translation by P map τ_P fits into the following commutative diagrams.

$$\begin{tikzcd}
E_1 \arrow[rr, "\tau_P"] \arrow[dr, "\phi"'] & & E_1 \arrow[dl, "\phi"] & \rightsquigarrow & k(E_1) & & k(E_1) \arrow[ll, "\tau_P^*"'] \\
& E_2 & & & & E_2 \arrow[ul, "\phi"] \arrow[ur, "\phi"'] &
\end{tikzcd}$$

Therefore, τ_P^* is an automorphism of $k(E_1)$ that preserves $k(E_2)$. Since there are exactly $\ker\phi = \deg\phi$ many of these (by assumption) this implies $\ker\phi$ is the Galois group.

[1] The fact that we can do this relies on ϕ being a finite map. That is, the degree is finite. Otherwise, the norm map would not be defined.

[2] Usually when we say 'isogeny' we mean 'nonzero isogeny.' This will often be implicit the facts we present.

Remark. In fact, the diagrams above are in complete correspondence because the (contravariant) functor

$$\begin{array}{rcl} (\text{smooth curves}/k) & \longrightarrow & (\text{Fields of transc. deg 1 over } k) \\ C & \mapsto & k(C) \end{array}$$

is an equivalence of categories.

Corollary 7.1.1. *Let $\psi : E_1 \to E_2$ and $\phi : E_1 \to E_3$ be isogenies. Then* $\ker\phi \subset \ker\psi$ *if and only if ψ factors through ϕ.*

To say that ψ factors through ϕ means that there is a map $E_3 \to E_2$ making the following diagram commute.

$$\begin{tikzcd} E_1 \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & E_2 \\ & E_3 \arrow[ur, dashed] & \end{tikzcd}$$

Proof. The implication $\Longleftarrow$ is clear. We prove $\Longrightarrow$. On the level of function fields we have

$$\begin{tikzcd} k(E_1) & & k(E_2) \arrow[ll, hook'] \arrow[dl, hook, dashed] \\ & k(E_3) \arrow[ul, hook] & \end{tikzcd}$$

By the above and Galois theory, it follows that

$$\mathrm{Gal}(k(E_1)/k(E_2)) = \{\tau_P^*\}_{P\in\ker\psi} =: \tau_{\ker\psi}^*,$$

and

$$k(E_2) = k(E_1)^{\tau^*_{\ker\psi}} \qquad \text{and} \qquad k(E_3) = k(E_1)^{\tau^*_{\ker\phi}}.$$

Hence $\ker\phi \subset \ker\psi$. □

Corollary 7.1.2. *Let E be an elliptic curve with $\Psi \subset E$ a finite subgroup. Then there is a unique E' and a separable isogeny $\phi : E \to E'$ such that* $\ker\phi = \Psi$.

Remark. Since $id : E \to E$ and $[-1] : E \to E$ are different automorphisms of E (i.e. they have the same kernel) it's not the case that the isogeny ϕ of the corollary is unique.

Proof. The group τ_Ψ^* acts on $k(E)$. Let $K = k(E)^{\tau_\Psi^*}$ be the fixed field. (One needs to check that $K \neq k$, but this is simple and left to the student.) Thus K is a field of transcendence degree 1 over k. By the equivalence of categories mentioned above, this means there is a curve C/k such that $K = k(C)$, and thus a map $E \to C$. To complete the proof, need to see that $g(C) = 1$ (and define its origin to be the image of O_E.)

A consequence of the Riemann-Hurwitz formula is that $g(C) \leq g(E)$. More precisely, it implies that that

$$\chi(E) = \deg\phi\,\chi(C) \tag{7.1.1}$$

if and only if τ_Ψ^* acts freely, meaning that there is no non-identity element which has fixed points. Since it is a group of translations this is obvious. The Euler characteristic χ is $2g-2$, so the left hand side of (7.1.1) is zero for *any* ϕ, from which it follows that $g(C) = 1$. □

The upshot is that isogenous curves to E are in one-to-one correspondence with finite subgroups of E. The sequence

$$\begin{tikzcd} 0 \arrow[r] & F \arrow[r] & E \arrow[r, "\phi"] & E' \arrow[r] & 0 \end{tikzcd}$$

is exact. We often write $E' = E/F = E/\ker\phi$.

Exercise 7.1.3. Prove that there exist elliptic curves E_1 and E_2 over $\mathbb{C}$ that are not isogenous. (Hint: Use that $\mathbb{C}$ is uncountable.)

7.2. **Isogenies and the invariant differential.** Let $\phi : E_1 \to E_2$ be an isogeny and ω_{E_2} and invariant differential on E_2. Then $\phi^*(\omega_{E_2})$ is an invariant differential on E_1.

Suppose that $\psi : E_1 \to E_2$ is another isogeny. Then it is a fact that

$$\psi^*\omega_{E_2} + \phi^*\omega_{E_2} = (\psi+\phi)^*(\omega_{E_2}).$$

This is not just abstract nonsense. Nor is it trivial because the addition on the left hand side addition in the k vector space of holomorphic differentials $\Gamma(E_1, \Omega^1)$ and on the right hand side the addition is that given b the group law on the elliptic curve E_2.

We often use this fact when $E_1 = E_2$. Let ω be a differential on E, and $\phi \in \text{End}(E)$. Then $\phi^*\omega = c_\phi\omega$ for some constant c_ϕ. This gives a map $c : \text{End}(E) \to k$. The fact above tells us that c is actually a ring homomorphism.

7.3. **The dual isogeny.** Given $\phi : E_1 \to E_2$ we want to define $\phi^* : \text{Pic}^0(E_2) \to \text{Pic}^0(E_1)$. On the level of divisors it is defined by $\phi^*(P) = \phi^{-1}(P)$. Need to check that this sends principal divisors to principal divisors. Indeed, if $f \in k(E_2)$, we have the following diagram.

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] & E_2 \arrow[r, "f"] & \mathbb{P}^1 \end{tikzcd}$$

So $\phi^*(div(f)) = div(f \circ \phi)$. (Recall that *div* looks at the zeros and poles of a function. So the diagram says that the zeros (or poles) of $f \circ \phi$ are exactly the points whose image in E_2 are zeros (or poles) of ϕ.)

This gives us a canonically defined isogeny $\hat{\phi} : E_2 \to E_1$.

8. February 16, 2010

Given an isogeny ϕ, $\hat{\phi}$ is called the *dual isogeny.* Note that

$$\phi_*\phi^*(P) = \phi_*\left(\sum_{Q|\phi(Q)=P} Q\right) = \sum_{Q|\phi(Q)=P} \phi(Q) = \deg\phi Q.$$

We conclude that $\phi \circ \hat{\phi} = [\deg\phi]$.

Two facts:

- $\widehat{\phi\circ\psi} = \hat{\psi}\circ\hat{\phi}$
- $\widehat{\phi+\psi} = \hat{\phi}+\hat{\psi}$

The first of these is a formal exercise, the second is contentful—it says something about the algebraic geometry of $E_1 \times E_2$.

Proposition 8.0.1.
- $\widehat{[m]} = [m]$,
- $\deg[m] = m^2$.

Proof. We induct on m. Clearly, if $m = 1$ the statements are obviously true. Then

$$\begin{aligned} \widehat{[m+1]} &= \widehat{[m]+[1]} \\ &= \widehat{[m]} + \widehat{[1]} && \text{by fact above} \\ &= [m] + [1] && \text{the inductive hypothesis} \\ &= [m+1]. \end{aligned}$$

(One can also readily check the statement is true for $-m$.)

For the second statement, we have

$$[\deg m] = [m]\widehat{[m]} = [m][m] = [m^2].$$

An argument can now be made that this implies $\deg m = m^2$. □

Note that $\phi \circ \hat{\phi} = [\deg \phi]$.

Taking the dual of both sides: $\hat{\hat{\phi}} \circ \hat{\phi} = [\deg \phi]$. So $\phi \circ \hat{\phi} = \hat{\hat{\phi}} \circ \hat{\phi}$ which implies since the map is dominant that $\phi = \hat{\hat{\phi}}$. We conclude, in particular, that dualization is an involution on $\mathrm{End}(E)$.

Remark on similarities between $\mathrm{End}(E)$ and $\mathrm{End}(k^2) = M_2(k)$.

$\mathrm{End}(E)$	$\mathrm{End}(k^2)$
dual	adjugate
$[m]$	mI
deg	det

Note that dualization and adjugate are linear contravariant and self-transpose.

The fact that $\deg{[m]} = m^2$ implies in characteristic prime to m that $E[m] = \ker[m]$ has size m^2. More precisely, $\#E(\overline{\mathbb{Q}})[m] = m^2$. When $m = p$ is prime

$$E[p] = \mathbb{Z}/p \times \mathbb{Z}/p.$$

Basic group theory then implies that

$$E[m] = \mathbb{Z}/m \times \mathbb{Z}/m$$

in general.

What if $char(k) \mid m$? For example, suppose $char(k) = p$. We have remarked that $\# \ker[p] = \deg_s[p]$ and $\deg[p] = p^2 = \deg_s[p] \deg_i[p]$. It is impossible for $\deg_i[p]$ to be 1, so there are two possibilities:

- Supersingular: $\deg_i[p] = p^2$,
- Ordinary: $\deg_i[p] = 1$.

Note that $Frob_p : E \to E^{(p)}$ is purely inseparable of degree p. So $\widehat{Frob} \circ Frob = [p]$. From this the claim above that $\deg_i[p] > 1$ follows. We conclude, moreover, that the inseparability of $[p]$ is determined by whether or not $\widehat{Frob}$ is separable.

Fact: $\deg_i : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive definite quadratic form. That it is positive definite is easy. That it is a quadratic form means that

$$\deg(\phi + \psi) - \deg \phi - \deg \psi$$

is linear in ϕ and ψ. We check

$$\begin{aligned}[\deg(\phi+\psi)]-[\deg\phi]-[\deg\psi] =&(\phi+\psi)(\widehat{\phi+\psi})-\phi\hat{\phi}-\psi\hat{\psi}\\ =&(\phi\hat{\phi}+\phi\hat{\psi}+\psi\hat{\phi}+\psi\hat{\psi})-\phi\hat{\phi}-\psi\hat{\psi}\\ =&\phi\hat{\psi}+\psi\hat{\phi}.\end{aligned}$$

So indeed it is bilinear.

Exercise 8.0.2. Let $E: y^2=x^3-x$. Note that $[i]:(x,y)\mapsto(-x,iy)$ is an isogeny defined over $\mathbb{Q}(i)$. Hence there is a map $\mathbb{Z}[i]\to\mathrm{End}(E)$. Describe the quadratic form on $\mathbb{Z}[i]$ which sends $a+bi$ to $\deg(a+bi)$.

8.1. **Tate module and Galois representations.** If ℓ is a prime and E is an elliptic curve over $\mathbb{Q}$ then we have seen that $E[\ell]=E(\overline{\mathbb{Q}})[\ell]=E[\ell](\overline{\mathbb{Q}})$ is a finite group isomorphic to $\mathbb{Z}/\ell\times\mathbb{Z}/\ell$.

Suppose that $P\in E[\ell]$ and $\sigma\in G_{\mathbb{Q}}=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $[\ell]P=O$. Moreover, since $G_{\mathbb{Q}}$ acts on $E(\overline{\mathbb{Q}})$ by group homomorphisms[3], $P^\sigma\in E[\ell]$ as well. This gives a representation

$$\rho_{E,\ell}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{Aut}(E[l])\subset\mathrm{GL}(E[\ell])\simeq\mathrm{GL}_2(\mathbb{Z}/\ell).$$

Last year, in class field theory, we studied one-dimensional representations of $G_{\mathbb{Q}}$. Elliptic curves give a method of studying 2-dimensional representations.

9. February 18, 2010

Last time we studied $E[p]=E[p](\overline{k})$, and discovered that when $p\neq$ the characteristic of k then

$$E[p]\simeq\mathbb{Z}/p\times\mathbb{Z}/p$$

as an abelian group.

9.1. **The Weil pairing.** Today we will examine a deeper structure on $E[m]$. For simplicity of exposition, we will assume that $char(k)\nmid m$. The Weil pairing is an alternating pairing

$$e:E[m]\times E[m]\to\mu_m.$$

To define this let $P\in E[m]$. Because $mP=0$, the divisor $m(P-O)$ must be principal say $div(f)=m(P-O)$ where $f\in k(E)^\times$. Let $P'\in E[m^2]$ be any point such that $mP'=P$. (We know such a P' exists because we know the structure of $E[m^2]$ from last time.) Now let

$$D=\sum_{R\in E[m]}([P'+_E R]-[R])$$

Note that $D=m^2P'-m^2O$ as an element of $\mathrm{Pic}^0(E)$ and so it is principal, say $div(g)$.

On the other hand,

$$\begin{aligned}div(f\circ[m])=&m\sum_{R\in E[m]}[P'+R]-m\sum_{R\in E[m]}[R]\\ =&mD=m\cdot div(g)=div(g^m).\end{aligned}$$

[3] The fact that $(P+Q)^\sigma=P^\sigma+Q^\sigma$ is a consequence of the fact that the group law is defined over $\mathbb{Q}$.

Hence $g^m = cf \circ [m]$.

Now let Q be another point in $E[m]$. Define $h \in k(E)^\times$ by

$$h(X) = \frac{g(X+Q)}{g(X)}.$$

By the above,

$$h(X)^m = \frac{g(X+Q)^n}{g(X)^n} = \frac{f([m](X+Q))}{f([m]X)} = \frac{f([m]X)}{f([m]X)} = 1.$$

Therefore, h is independent of X and $h(X) = e(P,Q) = \langle P, Q\rangle$ is an mth root of unity.

Properties of the Weil pairing.

1. e is bilinear: $e(P_1+P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1+Q_2) = e(P, Q_1)e(P, Q_2)$.
2. e is alternating: $e(P,P) = 1$.
3. e is non-degenerate: if $e(P,Q) = 1$ for all $Q \in E[m]$ then $P = O$.
4. e commutes with Galois action: $e(P^\sigma, Q^\sigma) = e(P,Q)^\sigma$ for all $\sigma \in G_k$.

Proof. (1) In the second variable we compute directly

$$e(P, Q+R) = \frac{g_P(X+Q+R)}{g_P(X)} = \frac{g_P(X+Q+R)}{g_P(X+R)}\frac{g_P(X+R)}{g_P(X)} = e(P,Q)e(P,R).$$

To compute $e(P+Q, R)$, let ϕ be a function with divisor $[P+Q]-[P]-[Q]+[O]$ (which is clearly principal.) Since

$$div(f_P) = mP - mO, \qquad div(f_Q) = mQ - mO, \qquad div(f_{P+Q}) = m(P+Q) - mO,$$

it follows that

$$div\left(\frac{f_{P+Q}}{f_P}\right) = m \cdot div(\phi) = div(\phi^m)$$

and thus that $f_{P+Q} = cf_p f_Q \phi^m$. So

$$\begin{aligned} f_{P+Q} \circ [m] =& c(f_P \circ [m])(f_Q \circ [m])(\phi \circ [m])^m \\ g_{P+Q}^m =& c g_P^m g_Q^m (\phi \circ [m])^m \end{aligned}$$

Now we compute

$$\begin{aligned} e(P+Q, R) =& \frac{g_{P+Q}(X+R)}{g_{P+Q}(X)} \\ =& \frac{g_{P+Q}(X+R)}{g_P(X)} \frac{g_{P+Q}(X+R)}{g_Q(X)} \frac{\phi([m](X+R)}{\phi([m]X)} \\ =& e(P,R) \cdot e(Q,R) \cdot 1. \end{aligned}$$

(2) Let τ_P denote the translation by P map. Choose P' such that $mP' = P$. Let

$$G = \prod_{i=0}^{m-1} g_P \circ \tau_{iP'}.$$

Recall that $div(g_P) = \sum_R [P'+R] - [R]$, meaning that g_P has poles ate $E[m]$ and zeroes at $P' + E[m]$. Therefore, G has zeroes at $iP' + E[m]$ for $i = 1, 2, \dots, m$ and poles at $iP' + E[m]$ for $i = 0, \dots, m-1$. Since the sets $iP' + E[m]$ coincide for $i = m$ and $i = 0$, it follows that $div(G) = 0$ and so G is constant. Hence

$$\prod_{i=0}^{m-1} g_P \circ \tau_{iP'} = G(X) = G(X + P') = \prod_{i=1}^{m} g_P \circ \tau_{iP'},$$

from which it follows that $g_P = g_P \circ \tau_P$ or, in other words, $g_P(X) = g_P(X + P)$. So $e(P, P) = \frac{g_P(X+P)}{g_P(X)} = 1$.

(3) Suppose $e(P, Q) = 1$ for all Q. Then $g_P(X + Q) = g_P(X)$ for all $Q \in E[m]$. So g_P is invariant under translation by $E[m]$. This means that under the map $[m] : E \to E$, g_P is in the fixed field of $k(E)$, i.e. $g_P = \phi \circ [m]$ for some $\phi : E \to \mathbb{P}^1$. So

$$cf \circ [m] = g_P^m = (\phi \circ [m])^m = \phi^m \circ [m].$$

and thus $\phi^m = cf$. Since $div(f) = mP - mO$, this implies that $div(\phi) = P - O$. We can conclude that $P = O$ because otherwise $\phi : E \to \mathbb{P}^1$ would be a degree 1 map, which is impossible.

(4) This is immediate since everything is defined over $\mathbb{Q}$. □

Note that (2) implies that $e(Q, P) = e(P, Q)^{-1}$. Indeed, combining with (1),

$$1 = e(P + Q, P + Q) = e(P, Q)e(P, P)e(Q, P)e(Q, Q) = e(P, Q)e(Q, P).$$

In characteristic 2, $e(P, P) = 1$ is stronger than $e(Q, P) = e(P, Q)^{-1}$.

One way to write the Weil pairing:

$$e : \wedge^2 E[m] = E[m] \otimes E[m]/\{P \otimes P \mid P \in E[m]\} \to \mu_\ell$$

9.2. **The Tate module.** The *Tate module* $T_\ell(E)$ of an elliptic curve E is $\varprojlim E[\ell^n]$.

Recall that if $\{A_i\}$ is a sequence of abelian groups together with homomorphisms

$$\cdots \to A_3 \xrightarrow{\phi_2} A_2 \xrightarrow{\phi_1} A_1 \xrightarrow{\phi_0} A_0$$

respecting composition then

$$\varprojlim_n A_n = \{(\dots, a_2, a_1, a_0) \mid \phi_{i-1}(a_i) = a_{i-1}\}.$$

It is an abelian group under coordinate-wise addition.

An example of a projective limit is the ℓ-adic integers $\mathbb{Z}_\ell$. The maps

$$\cdots \to \mathbb{Z}/\ell^3 \xrightarrow{\ell} \mathbb{Z}/\ell^2 \xrightarrow{\ell} \mathbb{Z}/\ell$$

lead to $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n$ which is a characteristic zero ring.

10. February 23, 2010

A *profinite group* is any group which can be written as the inverse limit of finite groups. (Recall/note that an inverse limit really depends on the maps ϕ_i not just on the groups A_i.)

The Tate module $T_\ell E$ is the inverse limit of $E[\ell^n]$. We can compatibly choose isomorphisms $E[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ such that the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "{[\ell]}"] & E[\ell^n] \arrow[r, "{[\ell]}"] \arrow[d, "\simeq"] & E[\ell^{n-1}] \arrow[r, "{[\ell]}"] \arrow[d, "\simeq"] & \cdots \\
\cdots \arrow[r] & (\mathbb{Z}/\ell^n\mathbb{Z})^2 \arrow[r] & (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 \arrow[r] & \cdots
\end{tikzcd}$$

commutes. Therefore, as an abelian group $T_\ell E \simeq \mathbb{Z}_\ell^2$. However, the Tate module also carries an action of G_k.

Indeed, G_k action commutes with multiplication by $[\ell]$ so the following is commutative, and implies that G_k acts on the Tate module.

$$\begin{tikzcd}
\cdots \arrow[r, "{[\ell]}"] & E[\ell^n] \arrow[loop above, "G_k"] \arrow[r, "{[\ell]}"] & E[\ell^{n-1}] \arrow[loop above, "G_k"] \arrow[r, "{[\ell]}"] & \cdots
\end{tikzcd}$$

We write this action as

$$\rho_{E,\ell} : G_k \to \mathrm{GL}(T_\ell E) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

This is called the *ℓ-adic representation attached to E.*

Moreover, the action of G_k is compatible with the Weil pairing. Again, we have a commutative diagram:

$$\begin{tikzcd}
\cdots \arrow[r] & E[\ell^2] \times E[\ell^2] \arrow[r] \arrow[d, "e_{\ell^2}"] & E[\ell] \times E[\ell] \arrow[d, "e_\ell"] \\
\cdots \arrow[r] & \mu_{\ell^2} = \mathbb{G}_m[\ell^2] \arrow[r, "{[\ell]}"] & \mathbb{G}_m[\ell] = \mu_\ell
\end{tikzcd}$$

So the Weil pairing gives a map $T_\ell E \times T_\ell E \to \varprojlim \mu_{\ell^n} = T_\ell \mathbb{G}_m$.

You can't tell much about E from $E[\ell]$. For instance, suppose that $char(k) \neq 2$. Let $E : y^2 = x(x-1)(x-\lambda)$ and $E' : y^2 = x(x-1)(x-\lambda')$ where $\lambda, \lambda' \in K$. Then $E[2]$ and $E'[2]$ are isomorphic as abelian groups with bilinear pairing. Indeed, if $E : y^2 = f(x)$ then

$$E[2] = \{O, P_i = (\alpha_i, 0) \mid \alpha_i \text{ is a root of } f\}.$$

From the properties of the Weil pairing it is not hard to see that $e(O, P_i) = 1$ for all i and $e(P_i, P_j) = -1$ if $i \neq j$ and 1 otherwise. In the case of E and E' above, $E[2]$ and $E'[2]$ are even isomorphic as G_k-modules. However, in general, E and E' aren't isomorphic.

In contrast, if k is a finite field (or a number field) Tate (resp. Faltings) proved that $T_\ell E \simeq T_\ell E'$ if and only if E and E' are isogenous.

More generally, we can as what we can learn about the quadratic space $\mathrm{Hom}(E_1, E_2)$ from $E[\ell]$ and $T_\ell E$. Suppose $\phi : E_1 \to E_2$ is an isogeny (with everything defined over some field k.) Then ϕ induces a map $E_1[\ell] \to E_2[\ell]$ of G_k-modules, and this extends to a map $T_\ell E_1 \to T_\ell E_2$.

Theorem 10.0.1. *Suppose that $char(k) \neq \ell$. Then $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{G_k}(T_\ell E_1, T_\ell E_2)$ is injective.*

Remark. When k is a number field or a finite field the map on Hom spaces is an isomorphism. One can check that this implies the statement of Tate/Faltings above.

Remark. $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{G_k}(E_1[\ell], E_2[\ell])$ need not be injective. For example, take $E_1 = E_2 = E$ and $\phi = [\ell]$. Question:(optional exercise) What about $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z} \to \mathrm{Hom}_{G_k}(E_1[\ell], E_2[\ell])$?

Note that if A is an abelian group then $A \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z} \simeq A/\ell A$.

Corollary 10.0.2. $\mathrm{End}(E)$ *is a free abelian group of rank* ≤ 4.

Lemma 10.0.3. *Let M be a finitely generated submodule of* $\mathrm{Hom}(E_1, E_2)$*. Let M^{div} be the submodule of* $\mathrm{Hom}(E_1, E_2)$ *containing all ϕ such that $[m]\phi \in M$ for some $m \in \mathbb{Z}$. Then M^{div} is finitely generated.*

Note that this is not a general statement about finitely generated submodules in general. For example, if $M = \mathbb{Z} \subset \mathbb{R}$. Then $M^{div} = \mathbb{Q}$ which is not finitely generated.

In a word, the idea of the proof is that $\frac{1}{m}\phi$ is an isogeny for arbitrarily large m because the degree map prohibits it.

Proof. We have $M^{div} \subset M \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^r$ for some r. We claim that M^{div} is a discrete subgroup. Indeed

$$\{\phi \mid \deg \phi \leq 1, \phi \in M^{div}\} \subset \{\phi \mid \deg \phi < 1\} \cap \mathrm{Hom}(E_1, E_2) = \{0\}.$$

Since deg is a positive definite quadratic form the set $\{\phi \mid \deg \phi \leq 1\}$ is an open region. This proves the claim. Since a discrete subgroup of $\mathbb{R}^r$ is finitely generated this completes the proof. □

Proof of Theorem. Let $\phi \in \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ vanish at in $\mathrm{Hom}(T_\ell E_1, T_\ell E_2)$. Write $\phi = \sum \beta_i \psi_i$ $(i = 1, \ldots, n)$ a finite sum with $\beta_i \in \mathbb{Z}_\ell$ and $\psi_i \in \mathrm{Hom}(E_1, E_2)$. Let $M = \mathbb{Z}\psi_1 + \cdots \mathbb{Z}\psi_n$. Choose $\phi_1, \ldots, \phi_r$ a basis of M^{div} (which exists by the Lemma.)

So we can write $\phi = \sum \alpha_i \phi_i$ for some $\alpha_i \in \mathbb{Z}_\ell$. Choose $a_i \in \mathbb{Z}$ such that $a_i \equiv \alpha_i \pmod{\ell^e}$, and let $f = \sum a_i \phi_i \in \mathrm{Hom}(E_1, E_2)$. Then $f \equiv \phi \pmod{\ell^e}$. i.e. $f - \phi = \sum \gamma_i \phi_i$ such that $\gamma_i \in \ell^e \mathbb{Z}_\ell$. So $f - \phi$ kills $E[\ell^e]$ as does ϕ. Hence f kills $E[\ell^e]$. By Galois theory this means there exists $g \in \mathrm{Hom}(E_1, E_2)$ such that $f = [\ell^e] \circ g$. So $g = \sum b_i \phi_i$ with $b_i \in \mathbb{Z}$, hence $f = \sum \ell^e b_i \phi_i$. Hence $a_i = \ell^e b_i \implies a_i \equiv 0 \pmod{\ell^e} \implies \alpha_i \equiv 0 \pmod{\ell^e}$. Since this is true for arbitrary e we conclude that $\alpha_i = 0$ for all i and thus $\phi = 0$. □

Regarding finite generation of $\mathrm{Hom}(E_1, E_2)$: What we have shown implies that if M is a finitely generated subgroup of $\mathrm{Hom}(E_1, E_2)$ then $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ injects into $\mathrm{Hom}(T_\ell E_1, T_\ell E_2)$, and thus M has rank at most 4.

Now let M be a finitely generated subgroup of $\mathrm{Hom}(E_1, E_2)$ of maximal rank. (Such an M exists because the rank of M is bounded above by 4!) By the lemma, M^{div} is also finitely generated, so we can replace M with M^{div} (which clearly has the same rank as M.)

Now let $\phi \in \mathrm{Hom}(E_1, E_2)$ which is not in M^{div}. Then the module generated by M and ϕ has rank strictly greater than the rank of M, since any relation

$$a\phi + a_1 m_1 + \cdots + a_r m_r = 0$$

would imply that ϕ was in M^{div}. This contradicts the hypothesis that M had maximal rank among finitely generated subgroups of $\mathrm{Hom}(E_1, E_2)$.

11. February 25, 2010

11.1. **The endomorphism ring.** Let E/K be an elliptic curve, $\mathrm{End}(E) = \mathrm{End}_{\overline{K}}(E)$ is a ring with the following properties.

- It is a free $\mathbb{Z}$-module of rank at most 4.
- It has an anti-involution $\iota : \phi \mapsto \hat{\phi}$ which satisfies $\iota(\phi\psi) = \iota(\psi)\iota(\phi)$ and $\iota^2 = id$, and $\phi\iota(\phi) \in \mathbb{Z}_{\geq 0}$ and $\phi\iota(\phi) = 0$ if and only if $\phi = 0$.

Some examples of rings that satisfy these properties:

1. $\mathbb{Z}$, $\iota = id$.
2. $\mathbb{Z}[\sqrt{-d}]$ for $d \geq 0$. (Or $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ if $d \geq 0$ and $d \equiv 3 \pmod 4$.) ι equals complex conjugation.
3. $H = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ where $ijk = i^2 = j^2 = k^2 = -1$. More generally, orders in a quaternion algebra.

Exercise 11.1.1. Check that the Hurwitz quaternion algebra $H + \mathbb{Z}(\frac{i+j+k}{2})$ satisfies the properties above. (The main thing here is to show that $\phi\iota(\phi)$ is integral.)

In fact, these are the only examples. That is, $\mathrm{End}(E)$ is $\mathbb{Z}$, and order in $\mathcal{O}_F$ for some quadratic imaginary field F, or and order in a quaternion algebra.

An ring *order* of a ring R is finitely generated free $\mathbb{Z}$-submodule $R_0 \hookrightarrow R$ such that $R = R_0 \otimes_{\mathbb{Z}} \mathbb{Q}$.

We showed that $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(E)) \leq r$ by considering the action of $\mathrm{End}(E)$ on $T_\ell E$. We can also consider the action of $\mathrm{End}(E)$ on the (1-dimensional) $\overline{K}$ vector space of holomorphic differentials on E $H^0(E/\overline{K}, \Omega^1)$. The action is given by $\phi \cdot \omega = \phi^*(\omega)$. So we have a map

$$\mathrm{End}(E) \to \mathrm{End}_{\overline{K}}(H^0(E/\overline{K}, \Omega^1)) = \overline{K}.$$

What is the kernel of this map? i.e. for which $\phi \in \mathrm{End}(E)$ does $\phi^*\omega = 0$? In characteristic zero only $\phi = 0$ satisfies this property, so the map is injective, and, in particular, $\mathrm{End}(E)$ is commutative.

Remark. All commutative rings ($\mathbb{Z}$ or an order in a quadratic imaginary field) arise as $\mathrm{End}(E)$ for some E.

In characteristic p, $Frob^* = 0$ because $Frob$ is purely inseparable. To see that quaternion orders arise, we give an example. Let

$$E : y^2 = x^3 - x \qquad \text{over } \mathbb{F}_7.$$

We have seen before that $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E)$. Since $\deg(Frob) = 7 \neq a^2 + b^2$ for any $a, b \in \mathbb{Z}$ and $\mathbb{Z}[i]$ is maximal among orders of $\mathbb{Q}(i)$, we can conclude that $\mathrm{End}(E)$ must be an order in a quaternion algebra Q.

To determine which quaternion algebra Q is we let $\ell \neq 7$ be a prime. Then

$$Q \otimes \mathbb{Q}_\ell = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}(T_\ell E) \otimes \mathbb{Q}_\ell \simeq M_2(\mathbb{Q}_\ell).$$

Since the rank of Q is 4 this implies that $Q \otimes \mathbb{Q}_\ell \simeq M_2(\mathbb{Q}_\ell)$. When Q satisfies this, we say that Q *splits* at ℓ.

We still have to determine what happens at two more primes: $\{7, \infty\}$. At ∞, $Q \otimes \mathbb{Q}_\infty = Q \otimes \mathbb{R}$ can't be $M_2(\mathbb{R})$ because Q is positive definite. This leaves only 7. One way to see that Q doesn't split at 7 is by knowing that quaternion algebras don't split at an even number of places. A direct way of seeing this is to consider the map

$$\mathrm{End}(E) \to \mathrm{End}(H^0(E/\overline{K}, \Omega^1)) \simeq \overline{\mathbb{F}}_7.$$

The existence of this map implies that $Q \otimes \mathbb{Q}_7$ has a nontrivial two-sided ideal, and that, therefore, $Q \otimes \mathbb{Q}_7$ is not isomorphic to $M_2(\mathbb{Q}_7)$.

We say "Q is $\{7, \infty\}$."

11.2. **Elliptic curves over finite fields.** Given $E/\mathbb{F}_q$ the basic invariant is $\#E(\mathbb{F}_q)$. If $(q,6)=1$ then we can write $E : y^2 = f(x)$. A good heuristic is to think that for the q choices of x, the probability that $f(x)$ is a square is $1/2$. Since whenever $f(x)$ is a square there are two choices of y, one would expect there to be $q+1$ points on E (the 1 is the point at infinity.) Moreover, if one takes this heuristic further, it can be deduced that $\#E(\mathbb{F}_q) = q + 1 + \text{ error }$ where the error term should be bounded by $c\sqrt{q}$.

Theorem 11.2.1 (Hasse). $q+1-2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q+1+2\sqrt{q}$.

Lemma 11.2.2. $F-1$ *is separable.*

Proof. $(F-1)^*\omega = F^*\omega - [1]^*\omega = -\omega$. □

Let $F : E \to E$ be Frobenius. i.e. $F(x,y) = (x^q, y^q)$. Let $P = (x,y) \in E(\overline{\mathbb{F}}_q)$. Then $P \in E(\mathbb{F}_q)$ if and only if $FP = P$. So, using the lemma, we can conclude that

$$\begin{aligned}\#E(\mathbb{F}_q) =& \{P \in E(\overline{\mathbb{F}}_q) \mid (F-1)P = 0\} \\ =& \# \ker(F-1) = \deg_s(F-1) = \deg(F-1) \\ =& (F-1)\widehat{(F-1)} = F\hat{F} - (F+\hat{F}) + 1 = q+1-(F+\hat{F}).\end{aligned}$$

So, we see that Hasse's theorem is equivalent to $\left|F+\hat{F}\right| \leq 2\sqrt{q}$.

12. March 2, 2010

Proof of 11.2.1. We compute

$$\deg nF+m = (nF+m)(\widehat{nF+m}) = m^2F\hat{F} + mn(\underbrace{F+\hat{F}}_{a}) + n^2 = m^2q + mn(F+\hat{F}) + n^2.$$

Since deg is positive definite we know that this is non negative for any choice of $m,n \in \mathbb{Z}$. This means that $(mna)^2 - 4(m^2q)(n^2) \leq 0$. Simplifying this gives $|a| \leq 2\sqrt{q}$ as desired. □

Since $G_{\mathbb{F}_q}$ is procyclic, the representation $\rho_{E,\ell} : G_{\mathbb{F}_q} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is determined by the image of Frobenius. On the other hand, what can we say about the action of F on $T_\ell E$, i.e. $\rho_{E,\ell}(F) \in \mathrm{GL}_2(\mathbb{Z}_\ell)$?

We know $\det F$ equals the action of F on $T_\ell \mathbb{G}_m = \varprojlim \mu_{\ell^n}$ is raising to the q power (or multiplication by q in the group law on $\mathbb{G}_m$.) Since the action of $\hat{F}$ must satisfy $F\hat{F}$ acts by $qI = \det FI$, we conclude that $\hat{F}$ is the adjugate to F. Hence $F + \hat{F}$ acts by $\operatorname{tr} FI$.

By definition, we have $a = F + \hat{F}$ which is a "motivic description." The above discussion implies that $a = \operatorname{tr} \rho_{E,\ell}(F)$, an "$\ell$-adic description." Since tr doesn't depend on the choice of basis, a is independent of the choice of isomorphism $T_\ell E \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$.

Note that a priori $\operatorname{tr} \rho_{E,\ell}(F)$ is an ℓ-adic integer and dependant on ℓ, but the above implies that it is in fact an integer independent of ℓ. This is the first example of an "independence of ℓ" result.

12.1. **The Weil conjectures.** Given an elliptic curve $E/\mathbb{F}_q$ we have $\#E(\mathbb{F}_{q^n})$ for $n = 1, 2, \ldots$. More generally, if $X/\mathbb{F}_q$ is a smooth projective variety, then we define

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

Some examples: $X = pt$.

$$\begin{aligned} Z(pt/\mathbb{F}_q, T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n}\right) \\ &= \exp(-\log(1-T)) = \frac{1}{1-T}. \end{aligned}$$

$X = \mathbb{P}^1$:

$$\begin{aligned} Z(\mathbb{P}^1/\mathbb{F}_q, T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\#\mathbb{P}^1(\mathbb{F}_{q^n})}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{(q^n+1)T^n}{n}\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{(qT)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n}\right) \\ &= \exp(-\log(1-qT) - \log(1-T)) = \frac{1}{(1-T)(1-qT)}. \end{aligned}$$

$X = \mathbb{P}^n$: One can show that

$$Z(\mathbb{P}^n/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}.$$

Let us now look at the case $X = E$. We have

$$\#E(\mathbb{F}_{q^n}) = \deg(F^n - 1) = q^n + 1 - (F^n + \hat{F}^n).$$

If we let α, β be the eigenvalues of $\rho_{E,\ell}(F)$ then we know that $q = \alpha\beta$ and $a = \alpha + \beta$. Moreover, $F^n + \hat{F}^n = \alpha^n + \beta^n$. So

$$\begin{aligned} Z(E/\mathbb{F}_q, T) &= \exp\left(\sum_{n=1}^{\infty} \frac{1 + q^n - \alpha^n - \beta^n}{n} T^n\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} + \sum_{n=1}^{\infty} \frac{(qT)^n}{n} - \sum_{n=1}^{\infty} \frac{(\alpha T)^n}{n} - \sum_{n=1}^{\infty} \frac{(\beta T)^n}{n}\right) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1 - aT + qT^2}{(1-T)(1-qT)}. \end{aligned}$$

Again, although we have used the ℓ-adic Tate representation to define α and β, the final answer is independent of ℓ.

If X is a smooth projective variety of dimension n, the Weil conjectures say that

1. $Z(X, T)$ is a rational function of T with rational coefficients.
2. (Functional equation) There exists an integer ϵ such that
$$Z(X, q^{-n}T^{-1}) = \pm q^{n\epsilon/2} T^{\epsilon} Z(X, T).$$
3. (Riemann Hypothesis) $Z(X, T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)}$ with $P_0 = 1 - T$, $P_{2n} = 1 - q^nT$, and for all i $P_i(T) \in \mathbb{Z}[T]$ with all roots having archimedean absolute value 1.

We compute ϵ in the case $X = \mathbb{P}^n$.

$$\begin{aligned} Z(\mathbb{P}^n, q^{-n}T^{-1}) =& \frac{1}{(1-q^{-n}/T)(1-q^{-n+1}/T)\cdots(1-1/T)} \cdot \frac{T^{n+1}}{T^{n+1}} \\ =& \frac{T^{n+1}}{(T-q^{-n})(T-q^{-n+1})\cdots(T-1)} \cdot \frac{q^n q^{n-1}\cdots q}{q^n q^{n-1}\cdots q} \frac{(-1)^{n+1}}{(-1)^{n+1}} \\ =& (-1)^{n+1} q^{n(n+1)/2} T^{n+1} Z(\mathbb{P}^n, T). \end{aligned}$$

So $\epsilon = n+1$.

13. March 9, 2010

We remark that part 1 of the Weil conjectures was proven by Dwork, while part 3 was proven by Deligne using etale cohomology.

If we set $\zeta(s) = Z(X, q^{-s})$ then the functional equation relates $\zeta(s)$ and $\zeta(n - s)$, hence the terminology. Part 3 of the Weil conjectures is called the Reimann hypothesis when $n = 1$. To explain this, note that $Z(X,T) = 0$ if and only if $P_1(T) = 0$. Since the roots of $P_1(T)$ have absolute value $q^{-1/2}$ this means that which means that $\zeta(s) = 0$ implies that $|q^{-s}| = q^{-1/2}$ so $\mathrm{Re}(s) = 1/2$.

Hasse's theorem is equivalent to the Riemann hypothesis for elliptic curves $E/\mathbb{F}_q$. To see this, it suffices to show that for $P_1(T) = 1 - aT + qT^2 = (1-\alpha T)(1-\beta T)$ the numbers α and β are complex conjugates. If so, then $\overline{\alpha} = \beta$ and $|\alpha|\,|\beta| = q$ implies that $|\alpha| = |\beta| = q^{1/2}$. This will be the case if $a^2 - 4q \leq 0$, but this is exactly Hasse's theorem.

Remark: We proved stuff about a using the Tate module. More generally, when X is a smooth projective variety of dimension 1 (i.e. a curve) then $P_1(T)$ is the characteristic polynomial of the $Frob_q$ acting on $T_\ell Jac(X) \simeq \mathbb{Z}_\ell^{2g(X)}$. In this case, $\deg(P_1) = 2g$.

Remark: The zeros of $\zeta(s)$ are periodic on $\mathrm{Re}(s) = 1/2$. This is due to the fact that $T = q^{-s}$ so multiples of $2\pi i/\log(q)$ added to s don't change T. This is in contrast to the Riemann zeta function for which the zeros get less dense as $\mathrm{Im}(s) \to \infty$.

In general, $\deg(P_i) = \dim(H^i_{et}(X, \mathbb{Q}_\ell)$. This is equal to $\dim(H^i(X/\mathbb{C}, \mathbb{Q})$ if X is the reduction of a complex variety.

13.1. **Ordinariness and supersingularity.**

We assume that k is a field of characteristic p. Recall that E/k is supersingular if $\hat{F}$ is purely inseparable where $F : E \to E^{(p)}$ is the map $(x,y) \mapsto (x^p, y^p)$.

Theorem 13.1.1. *If E is supersingular then E is isomorphic over $\overline{k}$ to a curve defined over $\mathbb{F}_{p^2}$.*

Proof. Since $\hat{F}$ is purely inseparable the map $\hat{F} : E^{(p)} \to E$ must factor through F. In other words, there is a map $\phi : E^{(p^2)} \to E$ such that the following diagram commutes.

$$\begin{tikzcd} E \arrow[r, "F"] & E^{(p)} \arrow[r, "\hat{F}"] \arrow[d, "F"'] & E \\ & E \arrow[ur, "\phi"'] & \end{tikzcd}$$

By analyzing the degrees, one finds that $\deg(\phi) = 1$, hence ϕ is an isomorphism. Thus $j(E) = j(E^{(p^2)}) = j(E)^{p^2}$, so $j(E) \in \mathbb{F}_{p^2}$. □

It is not hard to check that if $k = \mathbb{F}_q(T)$ then $Ty^2 = f(x)$ and $y^2 = f(x)$ have the same j-invariant but they are not isomorphic over $\overline{\mathbb{F}}_p$.

Theorem 13.1.2. *E is supersingular if and only if $\mathrm{End}_{\overline{k}}(E)$ has rank 4. If E is ordinary and k is finite then $\mathrm{End}_{\overline{k}}(E)$ has rank 2.*

We first prove the following.

Lemma 13.1.3. *If E' and E are isogenous then $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathrm{End}(E') \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Note that there are isogenous curves such that $\mathrm{End}(E) = \mathbb{Z}[i]$ and $\mathrm{End}(E') = \mathbb{Z}[2i]$.

Proof. Let $x \in \mathrm{End}(E)\otimes$ then the following diagram is commutative.

$$\begin{tikzcd}
E \arrow[r, "\phi"] \arrow[d, "x"'] & E' \arrow[d, dashed, "\phi x \phi'"] \\
E \arrow[r, "\phi"] & E'
\end{tikzcd}$$

where $\phi' = \hat{\phi} \otimes \frac{1}{\deg(\phi)}$. So the map $x \mapsto \phi' x \phi$ is an isomorphism. □

Proof of Theorem 13.1.2. Note that if M is an abelian group then $\mathrm{rk}_{\mathbb{Z}}(M) = \dim_{\mathbb{Q}}(M \otimes_{\mathbb{Z}} \mathbb{Q})$.

Suppose that $\mathrm{End}_{\overline{k}}(E)$ is an order in $K = \mathbb{Q}(\sqrt{-d})$ and E is supersingular. Let $\ell \neq p$ be a prime that is inert in K, and let $\Phi_m \subset E$ be cyclic subgroups isomorphic to $\mathbb{Z}/\ell^m\mathbb{Z}$ satisfying

$$\Phi_1 \subset \cdots \subset \Phi_{m-1} \subset \Phi_m \subset \cdots .$$

Define $E_m = E/\Phi_m$, so we have $\phi_m : E \to E_m$ with kernel Φ_m. We have

$$[p]_{E_m} \circ \phi_m = \phi_m \circ [p]_E.$$

Since E is supersingular, $\deg_i [p] = p^2$. By the Lemma, this is true of both $[p]_E$ and $[p]_{E_m}$.

By the previous theorem there are only finitely many (at most p^2) isomorphism class of supersingular curves over $\overline{k}$. In particular, there exists m, n such that $E_m \simeq E_{m+n}$. Since $\Phi_m \subset \Phi_{m+n}$ and E_m has an endomorphism whose kernel is cyclic and isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$, there exists $\phi = \phi_{m,n}$ such that

$$\begin{tikzcd}
E \arrow[r, "\phi_m"] \arrow[dr, "\phi_{m+n}"'] & E_m \arrow[d, "\phi"] \\
& E_{m+n}
\end{tikzcd}$$

commutes. So $E_m \simeq E_{m+n}$ by ϕ.

As an element of $\mathrm{End}(E)$, $N_{K/\mathbb{Q}}(\phi) = \deg(\phi) = \ell^n$. Then $\phi = [\ell^{n/2}$ and n is even. However, this is a contradiction because $\ker\,[\ell^{n/2}] \simeq (\mathbb{Z}/\ell^{n/2})^2$.

Suppose now that $\mathrm{End}(E)$ has rank 4 and E is ordinary. Then $E[p] \simeq \mathbb{Z}/p$. In fact, $T_pE \simeq \mathbb{Z}_p$. Consider the map $\mathrm{End}(E) \to T_pE \simeq \mathbb{Z}_p$. Since, by assumption, $\mathrm{End}(E)$ is an order in a quaternion algebra, this cannot be injective. So there exists

$\alpha \in \mathrm{End}(E)$ such that α kills $E[p^k]$ for all k. Hence $\deg \alpha > \#E[p^k] = p^k$ for all k which is clearly impossible. □

Note that when E is ordinary, $\mathrm{End}(E) \hookrightarrow \mathbb{Z}_p$. We can conclude that K is a quadratic imaginary field in which p splits since the kernel is an ideal of norm p. This leads to the natural question of whether, if K is a quadratic imaginary field in which p splits, there is an elliptic curve $E/\mathbb{F}_q$ (ordinary) with $\mathrm{End}_{\overline{k}}(E) \subset K$. The answer is "yes" by work of Tate-Honda, Deuring, and others.

Recall that E is supersingular if and only if $\hat{F}$ is purely inseparable. This is equivalent to each of the following.

- $\hat{F}^*\omega = 0$,
- $(F + \hat{F})^*\omega = [a]^*\omega = 0$,
- The image of a in K (via the map $\mathbb{Z} \to K$, $1 \mapsto 1$) kills ω which is equivalent to $a \equiv 0 \pmod{p}$ or $p \mid a$.
- $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$

And if $q = p$ then $E/\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.

14. March 11, 2010

14.1. **Elliptic curves over $\mathbb{C}$ (What is $E(\mathbb{C})$?)** We know that $E : y^2 = f(x)$ where f is a polynomial of degree 3. We analyze the set of solutions as Riemann did. Think of it as the graph of $y = \sqrt{f(x)}$. The first approximation is then a cover by two copies of $\mathbb{C}$ (identified at the roots of $f(x)$.)

[Picture drawn of two copies of $\mathbb{C}$ above another $\mathbb{C}$ having 3 distinguished points (the roots of $f(x)$.) A loop around one of the points.]

It can't be that the preimage of the loop lies on one of the copies of $\mathbb{C}$. To illustrate this, let us take $f(x) = x(x-1)(x-2)$. Then we consider the preimage of a small loop around the origin. Parametrize the loop by $x = 0.01e^{2\pi i t}$. Then the preimages for several values of t are given in the following table.

t	y
0	$0.1, -0.1$
1/2	$0.1i, -0.1i$
1	$-0.1, 0.1$

At $t = 0$ and $t = 1$ we see that we get the same preimages, but their order is switched. This means that the preimage of the loop can't be a loop.

[Picture drawn of two copies of $\mathbb{C}$. A slit is cut between two of the points and a slit is cut between the third point and the point at infinity (moved to a point in the plane for visual convenience.) Crossing the slit moves from the top plane to the bottom, or vice versa.]

Since the 'planes' should really be copies of $\mathbb{CP}^1$ (i.e. spheres) the resulting object is two spheres each with two holes removed and then attached to each other along those circles. So, topologically, $E(\mathbb{C})$ is a torus, i.e. $S^1 \times S^1$.

The algebraic structure of $E(\mathbb{C})$ means it is a complex manifold. We'd like to see its structure as such. To do this we try to make a map $E \to \mathbb{C}$ by fixing an invariant differential ω. Then we consider

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

This is not well defined because there are lots of choices of paths and the value depends on the choice of path. To fix this, notice that if γ_1 and γ_2 are two paths then $\gamma_1\gamma_2^{-1}$ gives an element of $\pi_1(E(\mathbb{C}), O)$. If $\gamma_1\gamma_2^{-1}$ represents the trivial element in the fundamental group (i.e. it can be deformed to the constant loop) then

$$\int_{\gamma_1} \omega - \int_{\gamma_2} \omega = \int_{\gamma_1\gamma_2^{-1}} \omega = 0.$$

[Picture drawn of torus with points O and P connected by two paths (that aren't homotopy equivalent.)]

In other words, we have a map $\pi_1(E(\mathbb{C}), O) \to \mathbb{C}$ which is in fact a homomorphism of groups. Since $\pi_1(E(\mathbb{C}), O)$ is a free abelian group of rank 2 this restricts what Λ, its image in $\mathbb{C}$, can be. It turns out that the map is injective and Λ is a lattice. This means that Λ is a rank 2 discrete subgroup, or in other words a rank two subgroup not contained in any $z\mathbb{R}$.

So while the original map $E(\mathbb{C}) \to \mathbb{C}$ was not well defined, we now have a map $E(\mathbb{C}) \to \mathbb{C}/\Lambda$ which is. Moreover, it is an isomorphism of complex manifolds. So as a complex manifold, $E(\mathbb{C})$ is $\mathbb{C}/\Lambda$ for some lattice Λ.

From this description it is easy to see what $E[n](\mathbb{C})$ is without using any of the facts that we have previously proven. The first way is to see that in a fundamental domain for $\mathbb{C}/\Lambda$ (let w_1, w_2 be generators of Λ) the n-torsion is the n^2 points generated by w_1/n and w_2/n. [Picture drawn.]

Another purely algebraic way to see this is via the following diagram of exact sequences.

$$\begin{tikzcd}
0 \arrow[r] & \Lambda \arrow[r] \arrow[d, "\times n"] & \mathbb{C} \arrow[r] \arrow[d, "\times n"] & \mathbb{C}/\Lambda \arrow[r] \arrow[d, "\times n"] & 0 \\
0 \arrow[r] & \Lambda \arrow[r] & \mathbb{C} \arrow[r] & \mathbb{C}/\Lambda \arrow[r] & 0
\end{tikzcd}$$

The maps down are multiplication by n in the respective group. The snake lemma now implies that $\mathbb{C}/\Lambda[n] \simeq \Lambda/n\Lambda$ which is clearly isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

From this we may deduce that if E is defined over a number field K then $E(K)[n] \subset (\mathbb{Z}/n\mathbb{Z})^2$. Moreover, the Lefschetz principle implies that $E(\overline{\mathbb{Q}}) \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

A natural question is "which lattices are possible?" The answer is that all of them are. We now give an idea of how this is shown. First, note that our map $E \to \Lambda$ required a choice of invariant differential. Thus, as a map from the set of elliptic curves to lattices it is only defined up to multiplication by $\mathbb{C}^\times$, i.e. up to *homothety.*

The Weierstrass $\wp_\Lambda$-function is a map

$$\mathbb{C}/\Lambda \to \mathbb{C} \cup \{\infty\}$$

which satisfies

$$(\wp_\Lambda')^2 = 4\wp_\Lambda^3 + g_{4,\Lambda}\wp_\Lambda + g_{6,\Lambda}\wp_\Lambda.$$

This gives a map

$$\mathbb{C}/\Lambda \to \mathbb{CP}^2 \quad z \mapsto (\wp_\Lambda(z), \wp_\Lambda'(z))$$

whose image is the algebraic curve $E_\Lambda : y^2 = 4x^3 + g_{4,\Lambda}x + g_{6,\Lambda}$. In other words, we have a map $\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$.

The upshot of this is that there is a bijection

$$\left\{ \begin{array}{c} \text{homothety classes} \\ \text{of lattices } \Lambda \subset \mathbb{C} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes} \\ \text{of elliptic curves } E/\mathbb{C} \end{array} \right\}$$

One can view the left hand side as something related to "Hodge theory" and the right hand side as something to do with "Moduli spaces." A third bijection is $\mathbb{C}$ via the j-invariant, i.e. $E \mapsto j(E)$.

14.2. **The space of lattices.** We now discuss a fourth equivalent characterization of elliptic curves by describing the set of homothety classes of lattices. If Λ is a lattice then it is generated by two complex numbers z_1, z_2. However, this not unique.

$$\begin{aligned} \{(\Lambda, z_1, z_2) \mid \Lambda = \mathbb{Z}z_1 + \mathbb{Z}z_2\} =& \{(z_1, z_2) \mid z_1, z_2 \text{ are } \mathbb{R}\text{-linearly independent}\} \\ =& \mathrm{GL}_2(\mathbb{R}) \end{aligned}$$

Since we are interested in the space up to homothety we will restrict ourselves to covolume 1 lattices:

$$\{(z_1, z_2) \mid z_1, z_2 \text{ generate a covolume 1 lattice}\} = \mathrm{SL}_2(\mathbb{R})$$

A nice way to make this identification is $(a + bi, c + di) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Going to covolume 1 identifies lattices that differ by $\mathbb{R}^\times$, but we would like to identify those differing by $x + iy \in \mathbb{C}^\times$. One readily checks that this action on lattices is equivalent to multiplying $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ by $\left(\begin{smallmatrix} x & y \\ -x & y \end{smallmatrix}\right)$ on the right. In order for this to act on $\mathrm{SL}_2(\mathbb{R})$, $x + iy \in \mathbb{C}^{(1)}$, i.e. $x^2 + y^2 = 1$. This group is $\mathrm{SO}(2)$.

The final identification that we need to do is identify (z_1, z_2) with (z_1', z_2') if they generated the same lattice. This corresponds to left multiplication on $\mathrm{SL}_2(\mathbb{R})$ by elements of $\mathrm{SL}_2(\mathbb{Z})$.

We conclude that

$$\left\{ \begin{array}{c} \text{homothety classes} \\ \text{of lattices } \Lambda \subset \mathbb{C} \end{array} \right\} \leftrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2).$$

Remark: Traditionally, one makes this identification via the upper half plane $\mathcal{H}$. However, $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2) \simeq \mathbb{H}$, so this is indeed equivalent. We use this formulation because it is often the case in number theory that one is interested in $\Gamma\backslash G/K$ where G is a topological group Γ is a discrete subgroup and K is compact. This is evidently such a case.

15. March 16, 2010

In the derivation last time we used the group $\mathrm{SL}_2(\mathbb{R})$, but we could have used $\mathrm{GL}_2^+(\mathbb{R}) = \{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det g > 0\}$. It is easy to see that

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2) \simeq \mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{GL}_2^+(\mathbb{R})/\mathrm{GO}(2)$$

where $\mathrm{GO}(2) = \{\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})\}$.

As remarked last time

$$\mathrm{SL}_2(\mathbb{R})/SO(2) \simeq \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}.$$

This isomorphism is realized by the map $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \frac{ai+b}{ci+d}$.

This gives three realizations of the same space which we denote by $Y(1)$. (Sometimes one of these formulations is more useful than the other for specific applications.)

What does $Y(1)$ look like? We can draw a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z}) = \langle \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right) 1, \rangle$ on $\mathbb{H}$, [typical picture drawn with i and ω (a third root of unity) identified] but in this picture the sides are identified as well as points along the bottom arc. This makes the quotient space look like a large teardrop. [Picture drawn with comment that the open portion corresponds to $\mathrm{Im}(\tau) \to \infty$ and points corresponding to $\tau = i$ and $\tau = \omega$.] This certainly looks like $\mathbb{C}$ (as the j-invariant tells us it should.) Remark: $j(E_{\mathbb{Z}+\mathbb{Z}i}) = 0$ and $j(E_{\mathbb{Z}+\mathbb{Z}\omega}) = 1728$.

Locally, near i what does this quotient space look like? In a small neighborhood of i only the action of $\left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right) : \tau \mapsto -\frac{1}{\tau}$ is visible. So z is identified with

$$-\frac{1}{z+i} - i = i(1 - \frac{z}{i} + \ldots) - i.$$

Looking just at the tangent space, the higher order terms in the expansion above are zero, so the identification is $z \leftrightarrow -z$. In other words, near i the quotient is $\mathbb{C}/\{\pm 1\}$. This is isomorphic to $\mathbb{C}$ as a topological space, but not as a manifold. It is an example of what is called an *orbifold*.

15.1. **Level structures.** Let's consider the space

$$\{(E,T) \mid E/\mathbb{C} \text{ is an ell. curve }, T \in E[N] \text{ has exact order } N\}/\sim .$$

where $(E_1, T_1) \sim (E_2, T_2)$ if there is an isogeny $\phi : E_1 \to E_2$ such that $\phi(T_1) = T_2$. We can think of this space as

$$\{(\Lambda, T) \mid \Lambda \text{ is a lattice}, T \in \Lambda/n\Lambda \text{ has exact order } N\}/\text{homothety}.$$

When $N = 1$ (as we have seen), this space, denoted $Y_1(N)$, is

$$\mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}(2).$$

In general it is

$$\Gamma_1(N) \backslash \mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}(2)$$

where

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right) \pmod{N}\}.$$

Similarly if we replace T by $C \subset E[N]$ where C is cyclic of order N then one finds that the corresponding space is

$$\Gamma_0(N) \backslash \mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}(2)$$

where

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid N \mid c\}.$$

This space is denoted $Y_0(N)$.

In the case of pairs $(E, \phi : \Lambda/N\Lambda \to (\mathbb{Z}/N\mathbb{Z})^2)$, where ϕ is a given isomorphism, the resulting space is

$$\Gamma(N) \backslash \mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}(2)$$

where

$$\Gamma(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \pmod{N}\}.$$

This space is denoted $Y(N)$.

Notice that there are maps

$$Y(N) \to Y_1(N) \to Y(N) \to Y(1)$$

given by $(\Lambda, \phi) \mapsto (\Lambda, \phi^{-1}(1,0))$ and $(\Lambda, T) \mapsto (\Lambda, \langle T \rangle)$ and $(E, C) \mapsto E$.

It is a fact that these are algebraic curves, but this is far from obvious. We have that $Y(1) \simeq \mathbb{C}$ (ignoring orbifold issues.) However, $Y_0(N)$ is not isomorphic to $\mathbb{C}$ in general.

We now hint at how one establishes that these are algebraic curves. Besides the map $Y_0(N) \to Y(1)$ above (as Yoda says) "there is another." This is $(E, C) \mapsto E/C$. This gives a map

$$Y_0(N) \to \mathbb{C}^2 \qquad (E, C) \mapsto (j(E), j(E/C)).$$

There is an algebraic relation between $j(E)$ and $j(E/C)$ so actually the image lies on a curve in $\mathbb{C}^2$. (This isn't the end of the story because the map may not necessarily be injective, but this is certainly the idea of the first step.)

More generally, given M, N (coprime) we have a two maps $Y_0(MN) \to Y_0(N)$

$$\begin{aligned} f_1 :&(E, C_{MN}) \mapsto (E, C_N) \\ f_2 :&(E, C_{MN}) \mapsto (E/C_M, C_{MN}/C_M) \end{aligned}$$

where C_N (resp. C_M) is the unique subgroup of C_{MN} of order N (resp. order M.)

This gives a (Hecke) correspondence. A *correspondence* on a curve X is a curve $Z \subset X \times X$ which projects dominantly (over an algebraically closed field this means surjectivity) to each copy of X. Ours is given by

$$Y_0(MN) \xrightarrow{(f_1, f_2)} Y_0(N) \times Y_0(N).$$

One can think of a correspondence as a generalization of the graph of a function.

Consider $D \in \mathrm{Pic}^0(Y_0(N)) =: J_0(N)$. Our correspondence gives a homomorphism $T_M : J_0(N) \to J_0(N)$ as follows. Write $D = P_1 + \cdots + P_r - Q_1 - \cdots - Q_r$. Then

$$T_m(D) = f_2(f_1^{-1}(P_1)) + \cdots + f_2(f_1^{-1}(P_r)) - f_2(f_1^{-1}(Q_1)) - \cdots - f_2(f_1^{-1}(Q_r)).$$

More compactly, $T_m : J_0(N) \to J_0(N)$ is $T_m D = f_{2*} f_1^* D$. (Recall that the upper and lower star maps are well defined on Pic^0.)

15.2. **Modular forms.** A (weak) modular form F of weight k is a function on pairs (E, ω) of elliptic curves together with invariant differential such that

$$F(E, \lambda\omega) = \lambda^k F(E, \omega).$$

For elliptic curves over $\mathbb{C}$, we define $f(\tau) = F(\mathbb{C}/\Lambda_\tau, dz)$. Then

$$\begin{aligned} f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau) =&F(\mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}, dz) \\ =&F(\mathbb{C}/\mathbb{Z} + \mathbb{Z}\frac{a\tau + b}{c\tau + d}, dz) \\ =&F(\mathbb{C}/\mathbb{Z}(c\tau + d) + \mathbb{Z}(a\tau + b), (c\tau + d)dz) \\ =&F(\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau, (c\tau + d)dz) \\ =&(c\tau + d)^k F(\mathbb{C}/\Lambda_\tau, dz) \\ =&(c\tau + d)^k f(\tau). \end{aligned}$$

Therefore, $f(\tau + 1) = f(\tau)$. With the proper definition of F, f must be holomorphic on $\mathbb{C}$, hence Fourier analysis then gives that

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n q^n \qquad \text{where } q := e^{2\pi i \tau}. \tag{15.2.1}$$

An example is the j function:

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

16. March 18, 2010

We define the following power series.

$$s_3 = \sum_{n\geq 1} \frac{n^3 q^n}{1-q^n}, \qquad s_5 = \sum_{n\geq 1} \frac{n^5 q^n}{1-q^n}$$

One can check that the coefficient of q^m in S_k is $\sum_{d|m} d^k$. Moreover, the following belong to $\mathbb{Z}[[q]]$.

$$h_4 = -5s_3, \qquad h_6 = -(5s_3 + 7s_5)/12$$

Using these, one defines the *Tate curve*

$$E^{Tate} : y^2 + xy = x^3 + h_4 x + h_6. \tag{16.0.2}$$

We also take ω^{Tate} to be the invariant differential $\frac{dx}{2y+x}$.

What is interesting about this curve? If $\tau_0 \in \mathbb{H}$ then, on the one hand, we have $E = \mathbb{C}/\Lambda_\tau$. On the other hand, $q_0 = e^{2\pi i \tau_0}$ has absolute value, so one can see that the power series s_3, s_5 converge, and (16.0.2) defines an elliptic curve E' over $\mathbb{C}$. It turns out that

$$j(E) = j(E') = \frac{1}{q} + 744 + 196884q + \cdots$$

and so these are the same curves.

Let F be a (weak) modular form. Using the Tate curve we can define the *q-expansion of F* to be $F(E^{Tate}, \omega^{Tate}) \in \mathbb{Q}((q))$. Last time we saw that *if f is holomorphic* then f has a q-expansion as in (15.2.1). Hence the point of view we are adapting for modular forms (i.e. functions on pairs (E, ω)) can define a q-expansion without having to give the holomorphicity condition.

Let $\widetilde{h}_4$, $\widetilde{h}_6$ denote the coefficients of h_4, h_6 reduced modulo p, and define

$$\widetilde{E}_p^{Tate} : y^2 + xy = x^3 + \widetilde{h}_4 x + \widetilde{h}_6$$

which is defined over $\mathbb{F}_p((q))$. This is an elliptic curve. To see this, we remark that the discriminant of this Weierstrass equation is $\Delta = q\prod_{n\geq 1}(1-q^n)^{24} = q + \cdots$. So regardless of what p is, Δ is nonzero in $\mathbb{F}_p((q))$. We define the *q-expansion of F modulo p* to be $F(\widetilde{E}_p^{Tate}, \omega^{Tate})$.

For instance, there is a modular form H_p called the *Hasse invariant* such that $H_p(E) = 0$ if and only if E is supersingular.[4] Can check that the q-expansion of H_p is identically 1. This implies, in particular, that $\widetilde{E}_p^{Tate}$ is never supersingular.[5]

A *modular form* of weight k over a field F is a weak modular form of weight k whose q-expansion in $F((q))$ actually lies in $F[[q]]$. If furthermore the q-expansion lies in $qF[[q]]$, we call it a *cusp form.* (Remark that for higher level structures there are multiple cusps, and defining a modular (or cusp) form is more complicated.)

[4] Note that the vanishing of a modular is independent of the choice of invariant differential.

[5] Although over $\mathbb{C}$ every elliptic curve is isomorphic to a Tate curve, this phenomenon is not general.

16.1. **Elliptic curves over local fields.** Let R be a complete discrete valuation ring (dvr) with K its field of fractions, $\mathfrak{m}$ its maximal ideal, and $v : K^\times \to \mathbb{Z}$ the valuation. Examples include $k[[t]]$ where k is any field and K_π a finite extension of $\mathbb{Q}_p$.

What is an elliptic curve over R? You could say

$$E : y^2 + \cdots = x^3 + \cdots$$

where the coefficients $a_i \in R$ and $\Delta \neq 0$. However, you would like that when $R \to R'$ is any ring homomorphism then there should be a map $E(R) \to E(R')$. For $R' = k = R/\mathfrak{m}$ the resulting *reduced curve* $E(k)$ will not be an elliptic curve unless Δ does not belong to $\mathfrak{m}$, that is, $\Delta \in R^\times$.

This turns out to be much better, but one still has to be careful because the discriminant depends on the choice of Weierstrass equation. To rectify this, let E be an elliptic curve over K. A given Weiestrass equation is called *minimal* of if $v(\Delta)$ is minimal among all Weierstrass equations with $a_i \in R$. The discriminant of such an equation is also called *minimal* and may be denoted Δ_{min}.

Two (isomorphic) examples:

$$y^2 = x^3 + x + 1 \qquad y^2 = x^2 + 5^4 x + 5^6.$$

The first equation has $\Delta = -2^4 \cdot 31$. The second has $\Delta = -2^4 \cdot 5^{12} \cdot 31$. Over $\mathbb{Z}_5$, the first is minimal, the second isn't.

An elliptic curve over R is one over K such that $v(\Delta_{min}) = 0$.

Note that if $v(\Delta) < 12$ then $\Delta = \Delta_{min}$. Similarly, if $v(c_4) < 4$ or $v(c_6) < 6$ then $\Delta = \Delta_{min}$. In fact, if the residue characteristic is not 2 or 3 then $\Delta = \Delta_{min}$ if and only if either $v(\Delta) < 12$ or $v(c_4) < 4$. (This is exercise 7.1 of AEC.)

If the residue characteristic is 2 or 3 the story is more complicated, but it is completely understood via Tate's algorithm. For example, over $\mathbb{Q}_2$

$$y^2 = x^3 - 11x - 890 \tag{16.1.1}$$

is not minimal. It's discriminant is $-2^{12} \cdot 17^4$. However, it is visibly clear that $v(c_4) = v(11) = 0$. A minimal Weierstrass form for this curve is

$$y^2 + xy + y = x^3 - x^2 - x - 14. \tag{16.1.2}$$

Given a minimal Weiestrass form for an elliptic curve E/K, the curve $\widetilde{E}/k$ defined by reducing the coefficients modulo $\mathfrak{m}$ may be singular. Let $\widetilde{E}_{ns}$ denote the nonsingular locus. We can classify $\widetilde{E}_{ns}$ as follows.

- If $v(\Delta) =$ we say that E has *good reduction* or that E extends to an elliptic curve E/R. In this case, $\widetilde{E} = \widetilde{E}_{ns}$ is an elliptic curve over k.
- If $v(\Delta) > 0$ and $v(c_4) = 0$ we say E has *multiplicative reduction.* Then $\widetilde{E}$ is a nodal singular curve and $\widetilde{E}_{ns}(\overline{k}) \simeq \overline{k}^\times$.
- If $v(\Delta) > 0$ and $v(c_4) > 0$ we say E has *additive reduction.* Then $\widetilde{E}$ is a cuspidal cubic and $\widetilde{E}_{ns}(k) \simeq k$.

Multiplicative and additive reduction are both called *bad reduction.*

Returning to our example above in equations (16.1.1) and 16.1.2, gives an example of a curve which has multiplicative reduction over $\mathbb{Q}_{17}$ and good reduction over $\mathbb{Q}_2$.

17. March 23, 2010

17.1. **Motives.** There is not a definition of motive in that we can say a motive is ________, but we can say that ________ is a motive. Today we'll talk about a motive as a "system of realizations" as in Deligne's paper on $\mathbb{P}^1 - \{0, 1, \infty\}$. Two other senses in which motives are studied are as "objects cut out by correspondences on algebraic varieties over $\mathbb{C}$" and "ring of motives $K_0(Var_K)$." In the latter of these, scissors construction, motivic integration and connection with logic (model theory) are discussed.

17.1.1. *The motive of an elliptic curve.* What about an elliptic curve makes it a motive? A motive is a "linearization" of an algebraic variety. There are three (plus a fourth "crystalline" notion that we won't discuss today) ways one can obtain a vector space from $E/\mathbb{Q}$.

(1) (etale story) $T_\ell E = \varprojlim E[\ell^n]$ which is isomorphic as a group to $\mathbb{Z}_\ell^2$. Define $V_\ell E = \mathrm{Hom}(T_\ell E, \mathbb{Q}_\ell)$. This is a 2-dimensional vector space over $\mathbb{Q}_\ell$ with an action of $G_\mathbb{Q}$.

(2) (Betti story) Consider $E_\mathbb{C}/\mathbb{C}$. Recall that for each holomorphic differential ω on E, we have a map $\pi_1(E) \to \mathbb{C}$ given by $\gamma \mapsto \int_\gamma \omega \in \mathbb{C}$. Since $\pi_1(E)$ is abelian

$$\pi_1(E) = H_1(E, \mathbb{Z}) = \{\text{loops } \gamma \text{ on } E \text{ up to isotopy}\}.$$

Our second space is $\mathrm{Hom}(H_1(E, \mathbb{Z}), \mathbb{Q})$ which is a 2-dimensional $\mathbb{Q}$ vector space.

(3) (deRham story) We already have the space of invariant differentials on E: $H_0(E, \Omega_E^1)$. Over $\mathbb{C}$, deRham cohomology gives an exact sequence

$$0 \to H_0(E/\mathbb{C}, \Omega_E^1) \to H^1_{dR}(E/\mathbb{C}) \to H^1(E, \mathcal{O}_E) \to 0$$

and, moreover, $H^1(E, \mathcal{O}_E)$ is canonically isomorphic to $H_0(E/\mathbb{C}, \Omega_E^1) \oplus \overline{H_0(E/\mathbb{C}, \Omega_E^1)}$. The theory of deRham cohomology can be described algebraically, and one gets an exact sequence

$$0 \to H_0(E, \Omega_E^1) \to H^1_{dR}(E/\mathbb{Q}) \to H^1(E, \mathcal{O}_E) \to 0$$

of $\mathbb{Q}$ vector spaces. $H^1_{dR}(E/\mathbb{Q})$ is our final vector space. Note that this looks just like the exact sequence above, but there is no canonical splitting.

17.1.2. *Comparison maps.* Betti ↔ etale. Recall that we showed that $E[m](\overline{\mathbb{Q}}) \simeq \frac{1}{m}\Lambda/\Lambda \simeq \frac{1}{m}H_1(E, \mathbb{Z})/H_1(E, \mathbb{Z})$. Let $m = \ell^n$ and taking the inverse limit, we find

$$T_\ell E \xrightarrow{\sim} H_1(E(\mathbb{C}), \mathbb{Z}) \otimes_\mathbb{Z} \mathbb{Z}_\ell$$

Taking $\mathrm{Hom}(\cdot, \mathbb{Q}_\ell)$ yields

$$V_\ell E \xleftarrow[\sim]{} \mathrm{Hom}(H_1(E(\mathbb{C}), \mathbb{Z}), \mathbb{Q}_\ell) \simeq H^1_{Betti}(E(\mathbb{C}), \mathbb{Q}_\ell)$$

Betti ↔ deRham. We have seen a map

$$H_0(E, \Omega_E^1) \times H_1(E(\mathbb{C}), \mathbb{Z}) \to \mathbb{C} \qquad (\omega, \gamma) \mapsto \int_\gamma \omega.$$

Equivalently, we have a map

$$H^0(E, \Omega_E^1) \to \mathrm{Hom}(H_1(E(\mathbb{C}), \mathbb{Z}), \mathbb{C})$$

which can be extended to a map

$$H^1_{dR}(E) \to \mathrm{Hom}(H_1(E(\mathbb{C}), \mathbb{Z}), \mathbb{C})$$

Tensoring with $\mathbb{C}$ gives a natural isomorphism

$$H^1_{dR}(E) \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \mathrm{Hom}(H_1(E(\mathbb{C}), \mathbb{Z}), \mathbb{C}) \otimes \mathbb{C}.$$

Per Deligne, a motive M is (at least) a set of vector spaces $M_B/\mathbb{Q}$, $M_{dR}/\mathbb{C}$ and $M_\ell/\mathbb{Q}_\ell$ (for all primes ℓ) together with isomorphism

$$M_B \otimes \mathbb{Q}_\ell \xrightarrow[c_{B,\ell}]{\sim} M_\ell \qquad M_B \otimes \mathbb{C} \xrightarrow{\sim} M_{dR} \otimes \mathbb{C}.$$

What's more, $M_{dR} \otimes \mathbb{C}$ should have a filtration

$$M_{dR} = F_k M_{dR} \supset F_{k-1} M_{dR} \supset \cdots \supset F_0 M_{dR} \supset F_{-1} M_{dR} = 0.$$

The constant k is called the *weight* of the motive. This is called the *Hodge filtration.*

It should also be the case that for all but finitely many p the representation $G_{\mathbb{Q}} \to \mathrm{GL}(M_\ell)$ is *unramified* at p, and so the map $G_{Q_p} \to \mathrm{GL}(M_\ell)$ factors through $G_{\mathbb{Q}_p}/I_p \simeq G_{\mathbb{F}_p} = \overline{\langle Frob_p \rangle}$. In this case the representation is determined by the image of $Frob_p$. We require that the eigenvalues of this action are algebraic integers all with complex absolute value $p^{-k/2}$. (In the elliptic curve case this matches what we've proved with $k = 1$–the Riemann hypothesis.)

Theorem 17.1.1. *If $X/\mathbb{Q}$ is a smooth projective variety and $i \in \mathbb{Z}_{\geq 0}$ then there is a motive (in the sense above) $H^i(X)$ with*

$$H^i(X)_B = H^1(X(\mathbb{C}), \mathbb{Q}), \quad H^i(X)_{dR} = H^i_{dR}(X/\mathbb{Q}), \quad H^i(X)_\ell = H^i_{et}(X, \mathbb{Q}_\ell).$$

Recall that Faltings proved that $\mathrm{Hom}(V_\ell E_1, V_\ell E_2) \simeq \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$. It is not true that

$$\mathrm{Hom}(E_1, E_2) \simeq \mathrm{Hom}(H^1_{dR}(E_1), H^1_{dR}(E_2))$$

However, given $\phi \in \mathrm{Hom}(H^1_{dR}(E_1), H^1_{dR}(E_2))$ that is compatible with the isomorphisms to $H^i_B(E_j)$ one does have a correspondence just as in the Faltings theorem. (This may become an exercise if Jordan can work it out himself.)

17.1.3. *The Tate motive:* $\mathbb{Q}(1)$. We finish with an example other than an elliptic curve, namely $X = \mathbb{G}_m$. From homework we know $\omega = \frac{dz}{z}$ is an invariant differential. Also, $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ which clearly has $H^1(\mathbb{G}_m) = \mathbb{Z}$ generated by a loop around the origin γ. Then

$$M_B = \mathbb{Q} \cdot \gamma \quad \text{and} \quad M_{dR} = \mathbb{Q}\frac{dz}{z}.$$

We have seen in the homework that $M_\ell = \mathrm{Hom}(T_\ell \mathbb{G}_m, \mathbb{Q}_\ell)$ has $G_{\mathbb{Q}}$ acting by the inverse of the cyclotomic character. This is denoted $\mathbb{Q}(1)$.

Since $\int_\gamma \frac{dz}{z} = 2\pi i$, we could write $M_B = 2\pi i \mathbb{Q}$ and $M_{dR} = \mathbb{Q}$, and this gives the compatibility isomorphism.

We proved that $\wedge^2 V_\ell E = \mathbb{Q}_\ell(1)$ in the homework. This suggests that one should have a *motivic* isomorphism $\wedge^2 H^1(E) \to \mathbb{Q}(1)$. In particular, should have maps

$$\begin{tikzcd}
\wedge^2 V_\ell \arrow[r] \arrow[d, "\wedge^2 c_{B,dR}"'] & 2\pi i \mathbb{Q} \\
\wedge^2 H^1_{dR}(E, \mathbb{Q}) \otimes \mathbb{C} \arrow[r] & \mathbb{Q}
\end{tikzcd}$$

So the map $\wedge^2 c_{B,dR}$ should have determinant $2\pi i$. This is the content of exercise 6.? from AEC about *quasiperiods* in which one proves that

$$\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i.$$

18. April 6, 2010

Recall that a modular form of level N and weight k over a ring R (such that $N \in R^\times$) is a function F which to any triple $(E/S, \omega, C)$ assigns a value in S. Here, E is an elliptic curve over an R-algebra S, ω is an invariant differential and C is a cyclic group of order N. Moreover, we require that $F(E/S, \lambda\omega, C) = \lambda^k F(E/S, \omega, C)$ for all $\lambda \in S^\times$ and that $F(E_{Tate}, \omega_{Tate}, C_{Tate}) = \sum_{n\in\mathbb{Z}} a_n q^n$, the q-expansion of F, satisfies $a_n = 0$ for all $n < 0$ (at all of the cusps.) If, moreover, the constant term(s) are all zero, we call F a *cuspform*.

Holomorphically, if F is a form over $\mathbb{C}$, we define $f : \mathbb{H} \to \mathbb{C}$ by

$$f(\tau) = F(\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau, dz, 1/N\mathbb{Z}/\mathbb{Z}).$$

Recall that $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

We introduce the standard notation

$$g \left|_([\gamma] \; \tau\right) = (c\tau + d)^{-k} g(\gamma\tau),$$

and denote the set of actions by a group Γ under this operation by $[\Gamma]_k$. (Note that $f\,|_k[\gamma]\,|_k[\gamma'] = f\,|_k[\gamma\gamma']$, so this is indeed a group action.) Hence if g is a classical modular form of level N and weight k (i.e. an f as above coming from a form F) then it is fixed by $[\Gamma_0(N)]_k$.

We showed earlier that f is holomorphic, and, since $\left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, if we write $q = e^{2\pi i\tau}$ then $f(\tau) = \sum_{n\geq 0} a_n q^n$. However, a function of this form that is invariant by $[\Gamma_0(N)]_k$ need not be a modular form. A third condition is necessary which we now describe.

We say a function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of level N and weight k if

- f is holomorphic,
- $f\,|_=[\gamma]\; f$ for all $\gamma \in \Gamma_0(N)$,
- $f\,|_k[\gamma]$ has a q-expansion with no nonzero coefficients for negative powers of q for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

If furthermore, the q-expansions all have nonzero constant terms then f is called a cuspform.

The condition on the q-expansion of f says that as $q \to 0$ ($\mathrm{Im}(\tau) \to \infty$) $f(\tau)$ is bounded. The third condition means that f has similar behavior "at all of the cusps."

[Picture drawn of the fundamental domain $\mathcal{F}$ of the $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathbb{H}$ along with translates $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\mathcal{F}$ and $\alpha\mathcal{F}$.]

Let $\mathcal{G} = \mathcal{F} \cup \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\mathcal{F} \cup \alpha\mathcal{F}$. The following statements are equivalent.

- $\mathcal{G}$ is a fundamental domain for the action of $\Gamma_0(2)$.
- $S = \{1, \alpha, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\}$ forms a complete set of coset representatives for $\Gamma_0(2)\backslash\mathrm{SL}_2(\mathbb{Z})$.

To see why this is the case, suppose that $\gamma z, z \in \mathcal{G}$. Without loss of generality, we may assume that $z \in \mathcal{F}$. If $\gamma z \in \beta\mathcal{F}$ then $\beta^{-1}\gamma z \in \mathcal{F}$. So $\beta^{-1}\gamma = 1$. Therefore, $\beta \in S$ if and only if the elements represent distinct cosets in $\Gamma_0(2)\backslash\mathrm{SL}_2(\mathbb{Z})$. Furthermore, the set is a complete set of coset representatives is equivalent to the requirement that translates of $\mathcal{G}$ by $\Gamma_0(2)$ cover $\mathbb{H}$. Indeed, if $z \in \mathbb{H}$ then $\gamma z \in \mathcal{F}$ for some

$\gamma \in \mathrm{SL}_2(\mathbb{Z})$. So $\gamma = \beta\gamma'$ for some β in S if and only if S forms a complete set of cosets.

Remark: $[\Gamma_0(p) : \mathrm{SL}_2(\mathbb{Z})] = p + 1$. Why? We have the inclusions

$$\Gamma(p) \subset \Gamma_0(p) \subset \mathrm{SL}_2(\mathbb{Z})$$

where $\Gamma(p)$ is normal in each of the other two subgroups. Thus, modding out gives

$$1 \subset \{\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)\} \subset \mathrm{SL}_2(\mathbb{F}_p)$$

and the index of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to that of $B = \{\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)\}$ in $\mathrm{SL}_2(\mathbb{F}_p)$. Since $\mathrm{SL}_2(\mathbb{F}_p)$ acts transitively on lines in $\mathbb{F}_p^2$ and B is the stabilizer of $\left[\begin{smallmatrix} \mathbb{F}_p \\ 0 \end{smallmatrix}\right]$, this, in turn, is equal to the number of the lines inf $\mathbb{F}_p^2$. This is readily seen to be $p + 1$.

What happens to $f(\tau)$ as $\tau \to 0$? It turns out that $f\left|_k\left[\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right]\right.$ has a q-expansion of the right type is equivalent to f behaves itself as $\tau \to 0$.

To verify the third condition in the definition of modular forms, we need to check verify that $f\,|_k[\gamma]$ has the proper q-expansion. It suffices to check this for $\gamma \in \Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$, but a smaller set may be sufficient. How many γ need to be verified is the same as asking "how many cusps are there?"

If $\gamma_\infty \in \Gamma_\infty = \{\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)\}$ then $g\,|_k[\gamma_\infty]\,(\tau) = g(\tau + n)$ is bounded as $\mathrm{Im}\,\tau \to \infty$ if and only if $g(\tau)$ is. Thus it sufices to check $\gamma \in \Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})/\Gamma_\infty$. These are the "cusps."

For example, take $\Gamma_0(2)$. Let f be a modular form for $\Gamma_0(2)$, and set $g = f\left|_k\left[\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right]\right.$. If $\gamma \in \Gamma_0(N)$ then

$$g\,|_k[\gamma] = f\left|_k\left[\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right]\right.|_k[\gamma] = f\left|_k\left[\gamma^{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)}\right]\right.|_k\left[\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right].$$

If $\gamma \in \Gamma = \Gamma_0(2)^{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)}$ then this is equal to g, but $\Gamma_0(2)$ is not normal so this need not be the case.

In other words, g is a modular form not for $\Gamma_0(2)$ but rather the smaller group $\Gamma = \{\left(\begin{smallmatrix} * & \\ * & * \end{smallmatrix}\right) \mod 2\}$. So $g(\tau+1) \neq g(\tau)$, but since $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, $g(\tau + 2) = g(\tau)$ and if $q = e^{2\pi i z}$ then $g(\tau) = \sum_n a_n q^{n/2}$. The integer 2 is the width of the cusp.

In general, if $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup (meaning $\Gamma(N) \subset \Gamma$ for some N) then $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})/\Gamma_\infty$ consists of double cosets $D_1, \ldots, D_k$ where D_i consists of w_i cosets of $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$. There are k cusps with cusp i having width w_i. Another way of defining the width of a cusp $\gamma \in \Gamma\backslash\mathrm{SL}_2(\mathbb{Z})/\Gamma_\infty$ is as the smallest positive integer n such that $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma^\gamma$. For $\Gamma_0(p)$ there is one cusp (∞) of width 1 and one cups (0) of width p.

The q-expansion of f "at a cusp" is dependant on the choice of $\gamma \in \Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$ modulo Γ_∞. To see this note that $f\,|_k[\gamma\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)]\,(\tau) = f\,|_k[\gamma]\,(\tau+1)$. So if $\sum a_n q^{n/w}$ is the q-expansion of the first one then $\sum a_n e^{2\pi i(tau+1)n/w} = \sum a_n e^{2\pi i n/w} q^{n/w}$ is the q-expansion of the second. So the two q-expansions differ by twisting by a character.

19. April 8, 2010

19.1. **Modular curves.** Let $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$ where $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})/\pm I$. $Y_0(N)$ is a non-compact Riemann surface (missing cusps.) We must compactify.

The analytic approach to compactifying: Look at the region $-1/2 \leq \mathrm{Re}(z) \leq 1/2$, $\mathrm{Im}(z) > 1$. In the q variable this corresponds to $0 < |q| < e^{-2\pi}$. The map $z \mapsto q$ is an analytic isomorphism, so to compactify we just add $q = 0$. By symmetry, do the same at each cusp. This process gives $X_0(N)$. This surface might not have genus 0, and in the case $N = 2$ is has some elliptic/orbifold points.

Algebraic approach: We have two natural holomorphic functions on

$$Y_0(N) = \{(E/\mathbb{C}, C) \mid C \subset E \text{ is a cyclic subgroup of order } N\}/\sim .$$

Namely,

$$j : Y_0(N) \to \mathbb{C} \quad (E, C) \mapsto j(E), \qquad j' : Y_0(N) \to \mathbb{C} \quad (E, C) \mapsto j(E/C).$$

This gives a map $\Phi_N = (j, j') : Y_0(N) \to \mathbb{A}^2$. One can show that j and j' satisfy an algebraic relation $f(j, j') = 0$. (This is not obvious by pure thought.) In fact, Φ_N is generically one-to-one. Thus $\Phi_N(Y_0(N))$ is an affine algebraic curve in $\mathbb{A}^2$. Call it $C : f(x, y) = 0$. It could be singular, but there is a smooth compact algebraic curve $C_0/\mathbb{C}$ with $\mathbb{C}(C) = \mathbb{C}(C_0)$ (meaning their function fields coincide, hence C and C_0 are birationally equivalent.) $C_0 = X_0(N)$. Since this is a compact smooth curve birational to $Y_0(N)$, it must contain $Y_0(N)$.

The two approaches give the same $X_0(N)$. The relation $f \in \mathbb{Q}[x, y]$. In fact, f is defined over $\mathbb{Z}[1/N]$. Thus C descends to a curve defined over $\mathbb{Q}$, and we can take $X_0(N)/\mathbb{Q}$ to be the unique smooth proper curve over $\mathbb{Q}$ with function field $\mathbb{Q}(C)$. We remark that Shimura was the one to recognize that this stuff is defined over number fields.

So we have curves $X_0(N)/\mathbb{Q}$ with the property that for any $K/\mathbb{Q}$

$$\{P \in X_0(N)(K)\} \leftrightarrow \left\{ (E/K, C/K) \,\middle|\, \begin{array}{c} E \text{ is a generalized e.c.,} \\ C \subset E \text{ a cyclic subgrp of order } N \end{array} \right\}$$

By "generalized" we mean that at cusps we get a nodal/degenerate curve.

An example. Look for $E/\mathbb{Q}$ with $P \in E(\mathbb{Q})$, $0 \neq P \in E[523]$. (Note that 523 is prime.) Given such a pair, we have that $\langle P \rangle$ is defined over $\mathbb{Q}$, so $(E/\mathbb{Q}, \langle P \rangle/\mathbb{Q}) \in X_0(523)(\mathbb{Q})$. This curve has genus bigger than one. (It is approximately 523/12.) So it has only finitely many such $\mathbb{Q}$ points by Faltings. In fact, there aren't any. This is the idea behind Mazur's theorem that if E/Q has $C/\mathbb{Q}$ cyclic of prime order then $\#C < 163$.

19.2. **Returning to modular forms.**

Proposition 19.2.1. *Let $M_k(\Gamma_0(N))$ be the space of weight k modular forms for $\Gamma_0(N)$. then $\dim M_k(\Gamma_0(N))$ is finite.*

Proof. Let $f_0 \in M_k(\Gamma_0(N))$, $f_0 \neq 0$. Make a map

$$M_k(\Gamma_0(N)) \to \mathbb{C}(\Gamma_0(N)\backslash\mathbb{H}) \qquad f \mapsto \frac{f}{f_0}.$$

This is well defined because $f(\gamma\tau)/f_0(\gamma\tau) = f(\tau)/f_0(\tau)$ for all $\gamma \in \Gamma_0(N)$. Moreover, this extends to the cusps because we know that they are defined there.

Let $V \subset \mathbb{C}(X_0(N))$ be the image. ($V = \frac{1}{f_0} M_k(\Gamma_0(N))$.) So if $g = f/f_0$ write $\div f = D^+ - D^-$ where D^+ (resp. D^-) consists of the zeros (respectively, the poles) of g. Note that D^- is a subset of the zeros of f_0. Let $d = \deg f_0$ (the zeros of f_0.) It is finite.

Suppose that $\dim V > d+1$. Choose $P \in Y_0(N)$ where f_0 does not vanish. Look at the Tayler expansion of $g \in V$ at P is some variable w:

$$g = c_0 + c_1 w + c_2 w^2 + \cdots$$

Now consider the map $V \to \mathbb{C}^{d+1}$, $g \mapsto (c_0, \dots, c_d)$. Since $\dim V > d+1$, this has a nontrivial kernel. Take $g = c_{d+1}w^{d+1} + \cdots$ in the kernel, so that

$$\div g = (d+1)P + \cdots - \{\text{zeros of } f_0\}.$$

But this is a contradiction because $X_0(N)$ is compact and so $\deg g = 0$. □

Remark. $S_2(\Gamma_0(N))$ is especially nice. Note that

$$d(\gamma\tau) = d(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^{-2}d\tau.$$

Therefore, if $f \in S_2(\Gamma_0(N))$ then $f(\tau)d\tau$ is a holomorphic 1-form on $\mathbb{H}$ invariant by $\Gamma_0(N)$, so it is a holomorphic 1-form on $Y_0(N)$. What about at on $X_0(N)$? If $f(\tau) = \sum a_n q^n$, since $d\tau = d(\frac{1}{2\pi i}\log q) = \frac{1}{2\pi i}\frac{dq}{q}$, then $f(\tau)d\tau$ is holomorphic at the cusp if and only if f is a cuspform. Indeed, this gives a map from cuspforms to holomoprhic differentials

$$S_2(\Gamma_0(N)) \to H^0(X_0(N), \Omega^1) \qquad f \mapsto f(\tau)d\tau$$

that is actually an isomorphism. As a consequence $\dim S_2(\Gamma_0(N) = g(X_0(N))$.

For example take $N = 11$. One can check that $g(X_0(11)) = 1$, so it is an elliptic curve. Therefore, $S_2(\Gamma_0(11))$ is generated by a single f and $f(\tau)d\tau$ is the holomorphic differential on $X_0(11)$.

19.3. **Hecke operators.**

Given a modular form $f \in M_k(\Gamma_0(N))$ and an integer m prime to N, define a new modular form $T_m f \in M_k(\Gamma_0(N))$ by

$$T_m f(E, C_N) = \sum_{\substack{C_m \subset E \\ \text{cyclic}}} f(E/C_m, C_N/C_m).$$

Notice that since m, N are relatively prime, if $\phi : E \to E/C_m$ then $\phi(C_N) = C_N/C_m$ is still a subgroup of order N.

What are these? Fact: if f is a cusp form then so is $T_m f$. For example, if $N = 11$ then $T_m f = \lambda_m f$ because the space of cusp forms is 1-dimensional. Next time we will discuss what these λ_m are.

20. April 13, 2010

Last time we saw that if F is a modular form of level N and p is a prime such that $p \nmid N$,

$$T_p F(E, \omega, C_N) = \sum_{\substack{\phi: E \to E' \\ \deg \phi = p}} (\phi(E), \phi(\omega), \phi(C_N)).$$

This gives a map

$$T_p : M_k(\Gamma_0(N)) \to M_k(\Gamma_0(N))$$

which happens to satisfy $T_p T_\ell = T_\ell T_p$ for all primes p, ℓ.

Question (same as at the end of last time): What are these?

20.1. **Hecke correspondences.** The *Hecke correspondence* $T_p \subset X_0(N) \times X_0(N)$ is the subvariety parametrizing pairs

$$[(E, C_N), (\phi(E), \phi(C_N)]$$

with $\deg \phi = p$ as above. Looking at the fiber of over a point $[E] \in X_0(N)$ we see that there are $p+1$ points in $T_p \cap ([E] \times X_0(N))$ because there are exactly $p+1$ isogenies of degree p (corresponding to the $p+1$ subgroups of E–i.e. of $E[p]$–of order p.) Similarly, there are $p+1$ elements in $T_p \cap (X_0(N) \times [E])$. Hence T_p is a correspondence of degree $p+1$ in the first variable and $p+1$ in the second variable. We say *degree* of T_p is therefore $(p+1, p+1)$.

Remark. If $f : X_0(N) \to X_0(N)$ is a morphism, the *graph of f* Γ_f is the subvariety of points $(P, f(P))$. Given P there is exactly one point lying over it in Γ_f, and given $f(P)$ there are exactly $\deg f$ points. So the degree of Γ_f is $(1, p)$.

Suppose we have a correspondence C on an elliptic curve E. Denote the projection maps by π_1, π_2. Because E is a group, can construct a map

$$f_C : E \to E \qquad P \mapsto \sum \pi_2(\pi_1^{-1}(P)). \tag{20.1.1}$$

(We remark that we can arrange for this to be a morphism, i.e. such that $f_C(0) = 0$.) In particular, get an element of $\mathrm{End}(E)$.

Let us consider those N for which $X_0(N)$ is an elliptic curve. For simplicity with will take $N = 11$, but any N for which $X_0(N)$ has genus N would be the same, and for general N their is a similar theory. Using (20.1.1) we think of $T_p \in \mathrm{End}(X_0(11))$. This is some (algebraic) integer. Which?

Theorem 20.1.1 (Eichler-Shimura)**.** *$T_p = a_p$.*

We now describe why this is the case. Recall that a_p is related to the curve $X_0(11)/\mathbb{F}_p$. It is a fact (observed by Shimura) that that $X_0(N)$ can be defined over $\mathbb{Q}$. Indeed $X_0(11)$ can be given by the Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$.

Over $\mathbb{F}_p$, T_p should be consist of pairs (E, E') where $\phi : E \to E'$ is an isogeny of degree p. i.e. $E' = E/C_p$. However, it seems there's only 1 cyclic subgroup to use because

$$E[p] = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } E \text{ is ordinary,} \\ 1 & \text{if } E \text{ is supersingular.} \end{cases}$$

Question: What happens to the $p+1$ isogenies from E (over $\overline{\mathbb{Q}}$ or $\mathbb{C}$) when we reduce modulo p?

To get an idea of what is happening lets us look at the group μ_2 of square roots of unity. Over $\mathbb{Q}$ this consists of two points ± 1. But we should really think of μ_2 as, not the points, but rather the equation. That is μ_2 is the vanishing locus of $x^2 - 1$. (In algebraic geometry we write $\mathrm{Spec}\, \mathbb{Z}[x]/(x^2 - 1)$.) We can consider $\mu_2/\mathbb{F}_p$ for any prime. For most primes its points are ± 1, but if $p = 2$, the polynomial $x^2 - 1 = (x-1)^2$ which is a "double point," or a "thickened point."

The same type of phenomenon is occurring for T_p. Let us take $p = 2$ and $E/\mathbb{F}_p$ ordinary. Then $E[2]$ consists of four points and the reduction consists of two (thickened) points. [Picture drawn of four points in a square mapping to 2 thick points. Three more copies of this map with the subgroups of order 2 and their images circled.]

What does "modding out by the first subgroup" (i.e. the one which maps to a single thickened point) mean? Well, it should be an isogeny of degree 2 whose kernel consists of a single point. The map $Frob_2 : E \to E^{(2)}$ is such a map. For general p, Γ_{Frob_p} is a subvariety in $T_p \subset (X_0(11)/\mathbb{F}_p)^2$ of degree $(1, p)$.

On the other hand, the set of pairs (E^p, E) lie on T_p as well since $\widehat{Frob_p} : E^{(p)} \to E$. This subvariety has degree $(p, 1)$. The union of this and Γ_{Frob_p} has degree $(p+1, p+1)$ and so it must be all of T_p.

(At this point Ekin suggested that the intersection points are supersingular elliptic curves, but Jordan wasn't so sure...)

So as a correspondence, $T_p = Fr + \widehat{Fr}$ which is exactly a_p by definition!

20.2. **More on elliptic curves over local fields.** Let K_v be a nonarchimedean local field with residue field k_v. Let E/K_v be an elliptic curve and $\widetilde{E}/k_v$ the reduction of a minimal Weierstrass equation. If we write $\widetilde{E}_{ns}$ for the nonsingular locus of $\widetilde{E}$,

$$E \text{ has } \begin{cases} \text{good reduction} & \text{if } \widetilde{E}_{ns} = \widetilde{E}, \\ \text{multiplicative reduction} & \text{if } \widetilde{E}_{ns}(\overline{k}) \simeq \mathbb{G}_a(\overline{k}) = \overline{k}^\times, \\ \text{additive reduction} & \text{if } \widetilde{E}_{ns}(k) \simeq \mathbb{G}_a(k) = k. \end{cases}$$

We have a Galois representation

$$\overline{\rho}_{E,p} : G_{K_v} \to \mathrm{GL}(E[p]).$$

Let I_v denote the inertia subgroup[6] of G_{K_v}. Since the sequence

$$1 \to I_v \to G_{K_v} \to G_{k_v} \to 1$$

is exact, if $\overline{\rho}_{E,p} \mid I_v$ is trivial, in which case we say it is *unramified*, then $\overline{\rho}_{E,p}$ is determined by the action of G_{k_v} which in many cases (all of those of interest to us) is generated by a single element. In these cases, therefore, $\overline{\rho}_{E,p}$ is determined by a single matrix.

Proposition 20.2.1. *If E has good reduction and the characteristic of k_v is prime to m then $\overline{\rho}_{E,p} : G_{K_v} \to \mathrm{GL}(E[m])$ is unramified.*

The converse is not true.

Theorem 20.2.2 (Neron-Ogg-Shafarevich)**.** *Let K_v be a nonarchimedean local field and p a prime different form the residue characteristic of K_v. Denote by the $\rho_{E,P}$ the Galois representation of*

Since $\overline{\rho}_{E,p}$ is the composition of $\rho_{E,p}$ and the reduction map $\mathrm{GL}(T_pE) \to \mathrm{GL}(E[p])$, it is immediate that Proposition 20.2.1 follows from Theorem 20.2.2.

We will prove the proposition next time.

21. April 15, 2010

The main engine in proving Proposition 20.2.1 is the following sequence of groups. Let L_w/K_v be any finite extension and ℓ_w/k_v the corresponding extension of residue fields. Recall that $(m, p) = 1$ where p is the characteristic of k_v. Let $E^{ns}(\ell_w)$ denote

[6] Let $\mathbb{Q}_p^{nr}$ denote the maximal unramified extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. Then I_v is defined to be $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr})$. The exact sequence is a consequence of basic Galois theory and the fact that $\mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p) = G_{\mathbb{F}_p}$.

the set of smooth points of the reduced curve, and let p denote the reduction map. Define

$$E^0(L_w) = \{P \in E(L_w) \mid p(P) \in E^{ns}()\}, \text{and}$$

$$E^1(L_w) = \{P \in E(L_w) \mid p(P) = 0\}.$$

By definition,

$$E^1(L_w) \to E^0(L_w) \to E^{ns}(\ell_w)$$

is exact.

Moreover, the map $E^0(L_w) \to E^{ns}(\ell_w)$ is surjective. This requires the following fact from formal groups. Any torsion point in $E^1(L_w)$ has order a power of p. Taking $L_w = K_v(E[m])$, this says that $E^0(L_w)[m] \to E^{ns}(\ell_w)[m]$ is injective. Now, one can apply Hensel's Lemma to get surjectivity.

We remark that the content to Hensel's Lemma doesn't apply blindly. For example, $x^2 - p \in \mathbb{Q}_p[x]$ reduces to $x^2 \in \mathbb{F}_p[x]$ which has a solution. However, this solution does not lift to a solution in $\mathbb{Q}_p$ (because α were such a lift then $v(\alpha)$ would have to be $1/2$.) The necessary condition is smoothness.

Proof of Proposition 20.2.1. In the case that E has good reduction, $E^{ns}(\ell_w) = E(\ell_w)$ and $E^0(L_w) = E(L_w)$. So we get $E(L_w)[m] \hookrightarrow E(\ell_w)[m]$. Suppose that $\iota \in I_v$ acts nontrivially on $E[m]$, i.e. there exist P such that $i(P) \neq P$. By the definition of inertia, P and $i(P)$ reduce to the same thing modulo w.[7] This contradicts injectivity, hence we can conclude that I_v acts trivially. □

The absence of torsion in $E^1(L_w)$ arises from an identification of $E^1(L_w)$ with the L_w points of a certain *formal group.* We compare with the case of the multiplicative group $\mathbb{G}_m/\mathbb{Q}_p$ to give an idea of how this works. Let us assume $p > 2$. Again, we have a surjective reduction map

$$\mathbb{G}_m(\mathbb{Z}_p) \to \mathbb{F}_p$$

which gives an exact sequence

$$1 \to 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 1.$$

The key fact is that $1 + p\mathbb{Z}_p$ has no nontrivial torsion. One way to prove this is an "analytic" (or, more accurately, a formal power series) method. The map

$$T \mapsto \log(T) = \sum_n (-1)^n \frac{(T-1)^n}{n}$$

defines an isomorphism of groups $1 + p\mathbb{Z}_p \to \mathbb{Z}_p$. The map converges precisely because if $u \in 1 + p\mathbb{Z}_p$ then $v(u-1) \geq 1$, and so one sees that the power series above converges in $\mathbb{Q}_p$. That it is group homomorphism follows formally. (As power series $\log(ST) = \log(T) + \log(S)$.)

A similar "analytic" argument shows that $E^1(K_v)$ has a finite index subgroup isomorphic as a group to $\mathcal{O}_{K_v}$ with group law addition.

[7] The terminology *inertia* (meaning lazy or weak) describes I_v because these are the elements of G_{K_v} that don't move K_v around enough to change the valuation.

21.1. **Galois representations coming from elliptic curves over global fields and from points on such curves.** Let K be a global field. So K is a number field (a finite extension of $\mathbb{Q}$) or the function field of a curve over $\mathbb{F}_q$ (a finite extension of $\mathbb{F}_q(T)$.) We have defined

$$\overline{\rho}_{E,p} : G_K \to \mathrm{GL}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p).$$

Let v be a prime of K. We say E *has good reduction at* v if E/K_v has good reduction. E has good reduction at all but finitely many places. To see why, let $y^2 + \cdots = x^3 + \cdots$ be a Weierstrass equation for E. For all but finitely many primes, the discriminant $\Delta \in \mathcal{O}_{K_v}^\times$.

If $S = \{v \mid E$ has good reduction at $v\}$, $\overline{\rho}_{E,p}$ is unramified for all v not in $S \cup \{p\}$. Recall that we have an inclusion $I_v \subset G_{K_v} \hookrightarrow G_K$ that is unique up to conjugacy. Since being in the kernel of $\overline{\rho}_{E,p}$ is conjugacy invariant, this gives a well defined notion of being unramified.

We are aiming to prove

Theorem 21.1.1 (Mordell-Weil)**.** *$E(K)$ is a finitely generated abelian group. So $E(K) \simeq \mathbb{Z}^r \oplus$ finite grp.*

Remark. For a given S and a given finite group G there are only finitely many isomorphism classes of homomorphisms $G_K \to G$ which are unramified outside S. For example, $G = \mathbb{Z}/2\mathbb{Z}$ and $K = \mathbb{Q}$. A map $G_\mathbb{Q} \to \mathbb{Z}/2\mathbb{Z}$ is unramified outside $S = \{p_1, \ldots, p_r\}$ is a quadratic extension $L/\mathbb{Q}$ unramified (in the usual notion of algebraic number theory) outside of S. Say $L = \mathbb{Q}(\sqrt{d})$. Then this says that d has no prime factors other than $p_1, \ldots, p_r$. Since we can take d to be squarefree, we see there are on the order of 2^r such fields.

In general, $G_K \to G$ unramified outside S has kernel G_L where $L/\mathbb{Q}$ is Galois with group G and L is unramified outside S. In particular, L/K has degree $\#G$. What is $|D_{L/\mathbb{Q}}|$? We have

$$D_{L/\mathbb{Q}} = \prod_{p \in S} p^{\nu_p}$$

where ν_p is bounded in terms of p and $\#G$. So there is a bound $D(S, \#G)$ such that $|D_{L/\mathbb{Q}}| \leq D(S, \#G)$.

Theorem 21.1.2 (Hermite)**.** *For any n, X there are only finitely many number fields $L/\mathbb{Q}$ with $[L : \mathbb{Q}] = n$ and $|D_{L/\mathbb{Q}}| < X$.*

We have seen that given E can construct $\overline{\rho}_{E,p} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$. Can ask what about the converse: given $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$, is there $E/\mathbb{Q}$ such that $\rho = \overline{\rho}_{E,p}$? Suppose (since it is an obvious necessary condition) that $\det \rho$ is the cyclotomic character χ_p. Then the answer is 'yes' for $p = 2, 3, 5$ but 'no' for larger p. (Proven by Rubin-Silverberg in the 90s.)

We can describe why in the case $p = 2$. $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. Let G_L be the preimage of the group generated by a transposition. By Galois theory, this corresponds to a cubic extension L. Let $f(x)$ be the minimal polynomial of some $\alpha \in L$. Then $E : y^2 = f(x)$ has $\overline{\rho}_{E,p} = \rho$.

The answer is 'yes' for the analogous question about existence of modular forms with given mod p Galois representation. This is Serre's conjecture (recently proved.)

A few words aout Galois representations associated to points. Let E/K and $P \in E(K)$, p a prime. Choose $Q \in E(\overline{K})$ such that $pQ = P$. (Note that the set of such points is $Q + E[p]$ so this choice is not unique.) We can consider the permutation action of G_K on $Q + E[p]$. This is not a linear action, but it isn't arbitrary either.

22. April 20, 2010

22.1. **Riad's talk: Ranks of elliptic curves.** Let $E/\mathbb{Q}$ be an elliptic curve. So $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$, and $\Delta = 4a^3 + 27b^2 \neq 0$. Let $E(\mathbb{Q})$ be the group of rational points. The Mordell-Weil theorem says that $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tor}$. The integer $r = rank(E)$ is called the *rank* of E.

The subgroup $E(\mathbb{Q})_{tor}$, the subgroup of finite order elements, is well understood. There is a description of which groups can occur as $E(\mathbb{Q})_{tor}$ due to Mazur. Namely, it's one of the following fifteen groups:

$$\mathbb{Z}/n\mathbb{Z}(1 \leq n \leq 10, n = 12) \qquad \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}(1 \leq m \leq 4)$$

On the other hand, r is not well understood comparitively. For example, it is not known which integers can occur as ranks of elliptic curves. So how can we study r?

The idea of Birch and Swinnerton-Dyer is to pick a prime $p \nmid \Delta$ and reduce E modulo p: $\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}$, $\overline{a}, \overline{b} \in \mathbb{F}_p$. We know that $|\#E(\mathbb{F}_p) - (p + 1)| < 2\sqrt{p}$ by Hasse. So, the idea is, the larger $E(\mathbb{Q})$ is, the larger the $N_p = \#E(\mathbb{F}_p)$ should be on average as p varies. With this in mind, consider

$$\pi_E(X) = \prod_{\substack{p<X \\ p\nmid\Delta}} \frac{N_p}{p}.$$

Conjecture 22.1.1 (BSD)**.** $\pi_E \sim c_E \log(X)^{rank(E)}$.

This can be recast in terms of L-functions as follows. Define

$$L(s, E) = \prod_{p\nmid\Delta}(1 + a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|\Delta} l_p(s, E)^{-1}$$

where $a_p = N_p - (p+1)$ and $l_p(s, E)$ is a polynomial in p^{-s} such that $l_p(E, 1) \neq 0$. The Hasse bound implies that $L(s, E)$ converges for $\mathrm{Re}(s) > 3/2$, but let's formally plug in $s = 1$:

$$L(1, E) \text{ ``=''} \prod_{p\nmid\Delta} \frac{p}{N_p} \prod_{p\nmid\Delta} l_p(1, E).$$

So, if $L(1, E) \neq 0$ then the values of N_p shouldn't get too large, so the rank should be zero.

Conjecture 22.1.2 (BSD 2)**.** *The function $L(s, E)$ extends analytically to all of $\mathbb{C}$, and $\mathrm{ord}_{s=1} L(s, E) = rank(E)$.*

Theorem 22.1.3 (Wiles, and others)**.** *$L(E, s)$ extends analytically to $\mathbb{C}$.*

The case of CM elliptic curves was known beforehand due to Deuring.

Can complete $L(s, E)$ to $\Lambda(s, E)$ which satisfies

$$\Lambda(s, E) = \delta(E)\Lambda(E, 2 - s)$$

for some $\delta(E) \in \{\pm 1\}$ which is called the *root number.*

Theorem 22.1.4 (Gross-Zagier, Kolyvagin)**.** *If $L(1, E) \neq 0$ then $rank(E) = 0$. If $L(1, E) = 0$ and $L'(1, E) \neq 0$ then $rank(E) = 1$.*

This is why people care about vanishing of central values.

So how can we study the rank by studying the nonvanishing of $L(s,E)$ and $L'(s,E)$? We want to convert to the study of $L(s,f_E)$ where f_E is the modular form corresponding to E.

Theorem 22.1.5 (Taylor-Wiles, Breuil-Conrad-Darmon-T)**.** *If E is an elliptic curve over $\mathbb{Q}$ of conductor N, there is a new form $f_E \in S_2(\Gamma_0(N))$ such that $L(s,E) = L(f,s)$.*

The previous theorem (of Wiles, et al) is really a corollary of this result. For a reference on this material see "Rational points on modular elliptic curves" by H. Darmon on his website.

22.2. **Quadratic twists of elliptic curves.** Let D be a fundament discriminant. The *D-th quadratic twist of E* is the elliptic curve $E_D : Dy^2 = x^3 + ax + b$. We would like to study the variation of $rank(E_D)$ as $D \to \infty$.

Let $F = f_E = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ be the modular form attached to E via the theorem above. If $(D,N) = 1$ then the twist of F by χ_D, where χ_D be the Kronecker symbol, is

$$F \otimes \chi(z) = \sum_{n=1}^{\infty} \chi_D(n) a_n q^n,$$

and $L(s, F\otimes\chi) = \sum_{n=1}^{\infty} \chi_D(n) a_n n^{-s} = L(s, E_D)$.

Conjecture 22.2.1 (Goldfeld)**.** (G1) $\sum_{1\le|D|<X} \mathrm{ord}_{s=1} L(1, F\otimes\chi_D) \sim \frac{1}{2}\sum_{1\le|D|<X} 1$.

(G1') *The average rank*

$$A(E) = \lim_{X\to\infty} \frac{\sum_{1\le|D|<X} rank(E_D)}{\#\{1 \le |D| < X\}} = \frac{1}{2}.$$

(G2) $\{\#D \mid 1 \le |D| < X, L(1, F\otimes\chi_D) \ne 0\} \gg_F X$.

(G2') $\{\#D \mid 1 \le |D| < X, rank(E_D) \ne 0\} \gg_E X$.

Kevin James and N. Vatsal have proved (G2') for some choices of E.

Theorem 22.2.2 (Ono-Skinner)**.** $\#\{1 \le D < X, D \in P(\epsilon,\pi) \mid L(F\otimes\chi_D \ne 0\} \gg_F \frac{X}{\log X}$ *where $P(\epsilon,\pi)$ is an auxiliary set requiring minor constraints.*

Theorem 22.2.3 (Ono)**.** *Under mild conditions on F,*

$$\#\{1 \le D < X \mid L(F\otimes\chi_D \ne 0\} \gg_F \frac{X}{\log X^{1-\alpha(F)}}$$

where $\alpha(F) \in (0,1)$.

How is the proved?

Theorem 22.2.4 (Waldspurger)**.** *Let D_0 be $|D|$ if D is odd and $|D|/4$ if D is even. Let $F \in S_2(\Gamma_0(N))$. There exists an integer $M > 0$ with $N \mid M$, a Dirichlet character χ modulo $4M$, a nonzero number $\Omega)F \in \mathbb{C}$ and a nonzero eigenform $g_F \sum_{n=1}^{\infty} b_F(n) q^n \in S_{3/2}(\Gamma_0(4M), \chi)$ such that if $\delta(F(D) > 0$ then*

$$b_F(D_0)^2 = \begin{cases} \frac{\epsilon_D L(1, F\otimes\chi_D, 1) D_0^{1/2}}{\Omega_F} & \text{if } (D_0, 4M) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

where $\epsilon)D$ is algebraic.

Aside for rank 1: Without using Waldspurger for L' we have the following.

Theorem 22.2.5 (Perelli-Pomykala)**.** $\#\{1 \leq D < X \mid rank(E_D) = 1\} \gg_F X^{1-\epsilon}$.

22.3. **Congruent number curves.** Consider the congruent number curve $E_D^c : Dy^2 = x^3 - x$. The congruent number problem is to determine which integers are areas of right triangles with rational sides. It is a fact that D is a congruent number if and only if $rank(E_D^c) \geq 1$.

Heath-Brown has shown that a positive proportion of such twists have rank 0. In 2002 Silverberg and Rubin gave the following table.

D	$rank(E_D^c)$
1	0 (Fermat 1640)
5	1 (1937)
34	2 (1945)
1254	3
29274	4
205015206	5 (2000)
61471349610	(2000)

Theorem 22.3.1 (Tunnel, 1983)**.** $L(1, E_D^c) = \frac{(n-2m)^2 a\Omega}{16\sqrt{|D|}}$ *where* $a = 1$ *if* D *is even and* $a = 2$ *if* D *is odd and*

$$n = \#\{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 2ay^2 + 8z^2 = |D|/a\},$$

$$m = \#\{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 2ay^2 + 32z^2 = |D|/a\}$$

and $\Omega \sim 2.62$. *In particular,* $L(1, E_D^c) = 1$ *if and only if* $n = 2m$.

23. April 27, 2010

Let K be a global field, and E/K an elliptic curve. Let S be the set of primes of residue characteristic ℓ together with those for which E has good reduction. Last time (the time before Riad) we discussed the fact that $\overline{\rho}_{E,\ell} : G_K \to \mathrm{GL}(E[\ell])$ is unramified at all primes outside of S. Equivalently, the field $K(E[\ell])$ is unramified over K outside of S.

In order to study $E(K)$, we also began to discuss the homomorphism $\rho_{P,\ell} : G_K \to Sym(T)$ where $P \in E(K)$ and $T = [\ell]^{-1}P = Q + E[\ell]$ for some $Q \in E(\overline{K})$. If $\sigma \in G_K$ then

$$[\ell](Q^\sigma) = ([\ell]Q)^\sigma = P^\sigma = P.$$

Therefore, G_K acts on T.

Claim: $\rho_{P,\ell}$ is unramified outside of S. To prove this let $Q \in T$ and $\sigma \in I_v$. Then Q^σ and Q reduce modulo v to the same point of $E/\overline{k}_v$. Hence $Q^\sigma - Q$ reduces to the identity. But, $Q^\sigma - Q \in E[\ell]$ on which for $v \notin S$ the reduction is injective. Therefore, $Q^\sigma - Q$ is the identity. Since σ and Q were arbitrary, it follows that I_v acts trivially on T.

In particular, $K(T)/K$ is unramified outside S. Since $G_{K(T)}$ is the kernel of $\rho_{P,\ell}$ and $\#T = \ell^2$, the degree of $K(T)/K$ less than or equal to $(\ell^2)!$. (Actually, it's much smaller, but for our purposes the best bound isn't necessary.) By Hermite,

$$\boxed{\begin{array}{c}\text{there are only finitely many}\\ \text{extesnions of } K \text{ of degree} \leq \ell^2)!.\end{array}} \tag{23.0.1}$$

Enumerate the points of $E(K)$ in some way $P_1, P_2, \cdots$. Then we say $P \sim P'$ if $K(T(P)) = K(T(P'))$. So (23.0.1) implies that there are only finitely many equivalence classes. What can we say about P, P' if $P \sim P'$? It turns out that this answer is "not much." A slightly refined equivalence relation is better.

We say that P and P' are *torsor equivalent* ($P \sim_t P'$) if there exists a bijection $\alpha : T(P) \to T(P')$ such that

- for all $\sigma \in G_K$ and all $Q \in T(P)$, $\alpha(Q^\sigma) = \alpha(Q)^\sigma$;
- for all $x \in E[\ell]$ and all $Q \in T(P)$, $\alpha(Q + x) = \alpha(Q) + x$.

Note that by the first condition if $P \sim_t P'$ then $P \sim P'$. This is because $K(T(P))$ is the fixed field of σ such that $Q^\sigma = Q$ for all $Q \in T$. Since α commutes with the action of Galois $K(T(P'))$ must be this same field.

So we have, as maps of sets, the following coverings.

$$E(K) \to E(K)/\sim_t \to E(K)/\sim$$

Our claim is that the second map is finite to one (which would imply that there are finitely many torsor classes.)

To prove the claim, suppose that $L = K(T(P))$ is fixed. If $T = T(P')$ is in this equivalence class, T carries an action of $\mathrm{Gal}(L/K)$ and of $E[\ell]$. There are only finitely many possibilities for an action of $\mathrm{Gal}(L/K)$ and $E[\ell]$ on a finite set Σ of size ℓ^2. That is to say, even if you have infinitely many $\Sigma_1, \Sigma_2, \cdots$, they fall into finitely many equivalence classes where $\Sigma_i \sim \Sigma_j$ if there exists a bijection $\alpha : \Sigma_i \to \Sigma_j$ commuting with both actions.

What does it say about P, P' if $P \sim_t P'$? Take as given such a bijection $\alpha : T(P) \to T(P')$ and consider $\alpha(Q) - Q$.

Proposition 23.0.2. *$\alpha(Q) - Q \in E(K)$.*

Proof. Since the Galois action commutes with α, we have

$$(\alpha(Q) - Q)^\sigma = \alpha(Q)^\sigma - Q^\sigma = \alpha(Q^\sigma) - Q^\sigma.$$

On the other hand, $Q^\sigma - Q = x \in E[\ell]$. So

$$\alpha(Q^\sigma) - Q^\sigma = \alpha(Q^\sigma - x) - (Q^\sigma - x) = \alpha(Q) - Q.$$

□

Now we multiply by ℓ: $[\ell](\alpha(\mathbb{Q}) - Q) = P' - P \in \ell E(K)$. In other words, P and P' are equivalent in $E(K)/\ell E(K)$. Since there are only finitely many torsor equivalence classes in $E(K)$ there are only finitely many in $E(K)/\ell E(K)$ which implies the following.

Theorem 23.0.3 (Weak Mordell-Weil)**.** *$E(K)/\ell E(K)$ is finite for all primes ℓ.*

Note that an abelian can fail to be finitely generated in three essential ways:

(1) It has lots of free generators. (eg. $Z^{\mathbb{Z}}$)
(2) It has high divisibility. (eg. $\mathbb{Q}$)
(3) It has large torsion. (eg. $\bigoplus_p \mathbb{Z}\mathfrak{p}\mathbb{Z}$)

The weak Mordell-Weil theorem rules out the first possiblity, but not the second because $\mathbb{Q}/\ell\mathbb{Q} = 0$ (and hence is finite) for all primes ℓ, but $\mathbb{Q}$ is not finitely generated. We will rule out the second possibility next time using the theory of heights.

We can prove that $E(K)_{tor}$ is finite (ruling out the third possibility) in the following manner. Let v be the smallest place (i.e. $\#k_v = \#K_v/\mathcal{O}_{K_v} = q$ is minimal) such that E has good reduction at v. Thus $E(K)[\ell] \hookrightarrow E(k_v)[\ell]$. On the other hand, suppose that $\mathbb{Z}/\ell\mathbb{Z} \subset E(K)$ for arbitrarily large ℓ. Then combining these gives an injection $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E(k_v)[\ell]$ for arbitrarily large ℓ. But this is a contradiction to the Weil bound for large enough ℓ.

Note that the third case is that for which $E(K)$ fails to be finitely generated for more general K. For example, let $K = \overline{\mathbb{F}}_q(T)$. Then a curve like

$$E : y^2 = x^3 + tx + \frac{1-t}{5-t}$$

is an elliptic curve over K which satisfied the Mordell-Weil theorem. However,

$$E' : y^2 = x^3 + x + 1$$

does not. (It is a fact that non "isotrivial curves" do satisfy MW where "isotrivial" means that the curve is actually defined over $\overline{\mathbb{F}}_q$.)

23.1. **Upper bounds for ranks.** Given $E/\mathbb{Q}$ how can we get a decent upper bound for $rank(E(\mathbb{Q}))$? Take $\ell = 2$, so we'll study $E(\mathbb{Q})/2E(\mathbb{Q})$. Let $K = \mathbb{Q}(E[2])$. Choose $P \in E(\mathbb{Q})$ and $Q \in T(P) = [2]^{-1}P$. Now define

$$\zeta_P : G_K \to E[2] \qquad \zeta_P(\sigma) = Q^\sigma - Q.$$

This is well defined because if $x \in E[2]$ then $(Q+x)^\sigma - (Q+x) = Q^\sigma - Q + x^\sigma - x$. But $x^\sigma = x$. In fact, ζ_P is a homomorphism. We have seen that $Q^\sigma - Q$ is fixed by G_K. Therefore,

$$(Q^\sigma - Q) + (Q^\tau - Q) = (Q^\sigma - Q)^\tau + (Q^\tau - Q) = Q^{\sigma\tau} - Q.$$

Notice that $\mathrm{Hom}(G_K, \mathbb{Z}/2\mathbb{Z})$ is in bijection with both $K^\times/(K^\times)^2$ and quadratic extension of K. Given $d \in K^\times/(K^\times)^2$, the corresponding homomorphism is exactly that whose kernel is $K(\sqrt{d})$. Thus ζ_P can be thought of as an element of $(K^\times/(K^\times)^2)^2$. One can check that

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$$

is actually a homomorphism of abelian groups.

For the moment, assume that $K = \mathbb{Q}$. Let S be the set of bad primes plus 2. then $\zeta_P : G_\mathbb{Q} \to E[2]$ is unramified outside of S. Equivalently if $\zeta_P = (d_1, d_2) \in (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^2$ then $(d_i, p) = 1$ for all $p \notin S$. (We can take of d_1, d_2 to be squarefree integers.) We find there are at most $2^{\#S+1}$ choices for each d_i. Hence

$$\dim_{Z/2\mathbb{Z}} E(\mathbb{Q})/2E(\mathbb{Q}) \leq 2\#S + 2.$$

So, for example, if E has prime conductor ($\#S = 1$) then $rank(E(\mathbb{Q})/2E(\mathbb{Q})) \leq 4$. This is an example of what is called *2-descent*.

We have seen injectivity of the map

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \{\zeta_P\}.$$

The object on the right is called the mod 2 Selmer group. One may ask whether the map is surjective, and the answer is "no" in general. The difference is the Tate-Shafarevich group.

If $K \neq \mathbb{Q}$ then the same idea works only elements of $(K^\times/(K^\times)^2)^2$ are slightly more difficult to describe. But, again, one can show that there are only finitely many possibilities for ζ_P.

Remark: In this lecture we have been doing Galois cohomology without saying so.

24. April 29, 2010

Last time we proved the weak Mordell-Weil theorem which says that if K is a global field, and E/K is an elliptic curve then $E(K)/mE(K)$ is finite for all integers m. We want to leverage this to show that $E(K)$ is finitely generated.

As mentioned last time, the main problem is that we don't want $E(K)$ to be infinitely divisible. i.e. we want that there does not exist $P \in E(K)$ of infinite order such that $\frac{1}{2}P, \frac{1}{4}P, \frac{1}{8}P, \cdots$ all in $E(K)$. We'd like a notion of "complexity" of a point of $E(K)$ for which $[2]P$ is more complicated that P and such that there exist only finitely many point of $E(K)$ with bounded complexity. We do this via the theory of heights.

24.1. **Heights.**

Let K be a global field and $P = (X_0 : X_1 : \cdots : X_n) \in \mathbb{P}^n(K)$. Define

$$H(P) = \prod_v \max\{|X_0|_v, \dots, |X_n|_v\}.$$

This notion is well defined because if $\lambda \in K^\times$ then

$$\prod_v \max\{|\lambda X_0|_v, \dots, |\lambda X_n|_v\} = \prod_v |\lambda|_v \prod_v \max\{|X_0|_v, \dots, |X_n|_v\} = H(P)$$

by the product formula. Let $h(P) = \log H(P)$.

From now on we simplify the discussion by assuming $K = \mathbb{Q}$. In this case we may write $P = (X_0 : \cdots : X_n)$ such that the X_i are relatively prime integers. (Note that we are relying on the fact that $\mathbb{Z}$ is a PID.) If v is finite then, because the elements are relatively prime, $\max\{|X_i|_v\} = 1$. Therefore $H(P) = \max\{|X_i|_\infty\}$, and so it is obvious that there are only finitely many points of height less than B for any finite B.

Fact: Suppose $F : \mathbb{P}^n \to \mathbb{P}^n$ is a morphism of degree d. So $F = (f_0, f_1, \dots, f_n)$ with each f_i a homogeneous degree d polynomial such that they have no nontrivial common vanishing.[8] Then there exist constant C_F and c_F such that

$$c_F H(P)^d < H(F(P)) < C_F H(P)^d \quad \leftrightsquigarrow \quad h(F(P)) = dh(P) + o(1)$$

for all $P \in \mathbb{P}^n(K)$.

Why is this true? We may assume that $H(P)$ is a large as we want (since there are only finitely many exceptions which would influence the constants but not their existence.) Let m_F be the largest coefficient of all of the polynomials f_i. Write $P = (X_0 : \cdots : X_n)$ with the X_i relatively prime integers as above. Then X_i belongs to the interval $[-H(P), H(P)]$ and $f_i(X_0, \dots, X_n)$ has height at most $\binom{n+1}{d} m_F H(P)^d$.

To show the lower bound is more challenging. It passes through the Nullstellensatz which is famously non effective. So the problem is to rule out P very complicated but somehow f_i take very small values. By Nullstallensatz, since $f_0, \dots, f_n$ have no common vanishing, we can actually write that the ideal $(f_0, \dots, f_n)$ is the unit ideal. (Here, for sake of argument, we're subbing $X_i = 1$ and looking affinely.)

[8] Note that we need $n \leq m$ in order to satisfy the vanishing condition, unless $d = 0$ in which case constant maps work.

Thus there are polynomials g_i such that $g_0 f_0 + \cdots + g_n f_n = 1$. (Nullstellensatz doesn't say anything about the size of the coefficients of the g_i.)

In fact, the same result is true if we take any finite morphism of projective varieties $f : X \to Y$ of degree d. Here the height on $X \subset \mathbb{P}^n$ (or Y) is given by restricting the height on $\mathbb{P}^n$. This *is* dependant on the choice of embedding, but that is just the nature of height.

In particular, consider $[2] : E \to E$ with the embedding in projective space given by a Weiestrass equation. Then $\tau_Q : E \to E$ is the morphism $P \mapsto P + Q$, and so by the above

$$h(P+Q) > h(P) + c_Q$$

for some constant c_Q. However, because we are avoiding using the teminology "line bundles," this is slightly cheating. Everything would be okay except the morphism $[2]$ does not extend to a morphism on all of $\mathbb{P}^2$. The problem is that $[2] : O \to O$ but τ_Q does not. What is true is that

$$h(P+Q) - h(P) = o(h(P)).$$

So

$$(1+\epsilon)h(P) - c_Q < h(P+Q) < (1+\epsilon)h(P) + c_Q. \tag{24.1.1}$$

Given all this, how to prove the Mordell-Weil conjecture? Let $S = \{Q_1, \dots, Q_r\}$ be a set of representatives for $E(K)/mE(K)$. Let $P \in E(K)$, and define a sequence of points P_i such that

$$P = Q_{i_1} + mP_1, P_1 = Q_{i_2} + mP_2, \dots, P_{n-1} = Q_{i_n} + mP_n.$$

So $P_j = Q + mP_{j+1}$ for some $Q \in S$. Then (we take $\epsilon = 1$ in formula (24.1.1))

$$h(mP_{j+1}) < 2h(P_j) + c_Q, \qquad m^2 h(P_{j+1}) < 2h(P_j) + c_Q + C \implies h(P_{j+1}) < \frac{2}{m_2} h(P_j) + d.$$

Iterating this process, we may say that $h(P_{j+1}) < \frac{2}{m_2} h(P) + d$. Let R be the set of all such points in $E(K)$. Then $S \cup R$ is a finite generating set for $E(K)$.

24.2. Height over $\mathbb{F}_q(t)$.

A point $P \in \mathbb{P}^1(\mathbb{F}_q(t))$ may be written as $(f : g)$, and the absolute value $|f|_v = q^{-\operatorname{ord}_v(f)}$ where $\operatorname{ord}_v(f)$ is the order of vanishing (or pole) at $v \in \mathbb{P}^1(\mathbb{F}_q)$. Thus

$$h(P) = \log_q H(P) = \sum_v \max\{-\operatorname{ord}_v(f), -\operatorname{ord}_v(g)\}.$$

We can think of P as a morphism $\mathbb{P}^1 \to \mathbb{P}^1$ sending $(t : 1)$ to $(f(t) : g(t))$. As an exercise, check that $h(P)$ is the degree of this map. In particular, for this case, there are no difficult constants to consider when computing heights.

24.3. The canonical height.

Recall that $h([2]P) \sim 4h(P)$. So $h([2^n]P) \sim 4^n h(P)$, but the bound is even better. With this in mind, define the *canonical height*

$$\hat{h}(P) = h_{NT}(P) = \lim_{n\to\infty} \frac{h([2^n]P)}{4^n}.$$

It is hard to show, but true, that the set of points $\{P \in E(K) \mid \hat{h}(P) < B\}$ is finite, but it is easy to see that $\hat{h}([2]P) = 4\hat{h}(P)$. In fact, $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ is a positive definite quadratic form.

When $E(\mathbb{Q}) \simeq \mathbb{Z}$ and P is a generator then $\hat{h}(P)$ is related to $L'(1, E)$ by the Gross-Zagier formula.

Exercises

In addition to the exercises interspersed in the text, Jordan assigned the following. (The numbered problems come from AEC.)

- 1.1, 1.10 (see examples 2.3 and 2.5 for inspiration), 3.2, 3.3, 3.5. OPTIONAL algebraic geometry: 2.2, 2.3, 2.4, 2.7, 2.8, 2.11, 3.10, ...
- Differentials: Let k be a field, let $\mathbb{P}^1/k$ be the projective line over k, and let z be a coordinate on $\mathbb{P}^1$. $\mathbb{G}_m$ is what we call the variety obtained by removing the points $z = 0$ and $z = \infty$. from $\mathbb{P}^1$. Alternatively, we can think of $\mathbb{G}_m$ as the affine line with the point $z = 0$ removed, or, for the scheme fans, $Spec(k[z, u]/[uz - 1])$.

  Note that $\mathbb{G}_m$ is a GROUP SCHEME – that is, there is a morphism
  $$M : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$$
  which obeys the axioms of a group. This is just what you think: $M(z_1, z_2) = z_1 z_2$.
  (a) Describe the space of holomorphic differentials on $\mathbb{G}_m$. (That is: the space of differentials on $\mathbb{P}^1$ whose poles are all at either 0 or ∞.) Note that, by contrast with the case of elliptic curves, this is not a 1-dimensional or even finite-dimensional space! (Hint: every function f on $\mathbb{G}_m$ can be written as a polynomial in z and $u = 1/z$; it follows that every differential can be written as $P(z, 1/z)dz$ for some polynomial P.)
  (b) A *translation* in $\mathbb{G}_m$ is a map $t_a : \mathbb{G}_m \to \mathbb{G}_m$ sending z to az. You have a translation morphism t_a for each $a \in k^\times$. Describe the space of TRANSLATION-INVARIANT holomorphic differentials. In particular, show that (just as for elliptic curves) the space of invariant differentials is 1-dimensional, and that every nonzero invariant differential is not only holomorphic but everywhere nonzero.
- Write down an holomorphic, everywhere nonzero differential on the curve $X^3 + Y^3 + Z^3 = 0$. By the arguments made in class, such a differential must be translation-invariant, but you need not prove this.
- Modular forms: Recall the preliminary definition of modular form given in class: a (weak) modular form of weight k over a field K is an algebraic function f which – for each K-algebra L and each $(E, \omega)/L$, returns a value $f(E, \omega)$ in L satisfying
  $$f(E, \lambda\omega) = \lambda^{-k} f(E, \omega).$$
  Equivalently (I didn't prove this in class), f is an algebraic function of the coefficients of a Weierstrass form $(a_1, a_2, a_3, a_4, a_6)$ which is HOMOGENEOUS in the sense that
  $$F(a_1, a_2, a_3, a_4, a_6) = u^k F(a_1', a_2', a_3', a_4', a_6')$$
  where a_i' are related to a_i by a standard coordinate transformation, as in Table III.1.3 of Silverman. Show that a_1 is a modular form over the field $\mathbb{F}_2$, and b_2 is a modular form over the field $\mathbb{F}_2$ and also over $\mathbb{F}_3$.
- Isogenies: Write down an elliptic curve $E/\mathbb{Q}$ with a point $P \in E(\mathbb{Q})$ such that $[4]P = 0$. (Feel free to construct such a curve in any way you like except for looking it up.)
- 3.8, 3.12.

- 3.16, 3.17, 3.18, 3.20, 3.24.
- 2-torsion problems: Let K be a field of characteristic not equal to 2, and let E be an elliptic curve with equation $y^2 = f(x)$ with f a cubic polynomial.
  (a) Show that $f(x)$ is irreducible if and only if the mod 2 Galois representation $\overline{\rho}_{E,2}$ is irreducible.
  (b) Suppose K is a number field and let v be a prime of $\mathcal{O}_K$. Let Δ be the discriminant of E. Let I_v be the inertia group of G_K at v. Prove that the subgroup $\overline{\rho}_{E,2}(I_v)$ of $\mathrm{GL}(E[2])$ is a Borel subgroup if and only if $\mathrm{ord}_v(\Delta)$ is odd. (Note that, while Δ may depend on the choice of Weierstrass model, the parity of $\mathrm{ord}_v(\Delta)$ does not.) Possible counterexample due to Guillermo: Let $E : y^2 = x^3 - 3$ and $p = 3$. Here the image of inertia is the whole group $\mathrm{GL}(E[2])$ since $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{3})$ is a degree 6 extension of $\mathbb{Q}$ totally ramified at 6. On the other hand the valuation at 3 of the discriminant is 5, however the image is not Borel. The idea behind the example is that the valuation of the discriminant at a prime v is odd iff the image of inertia at v is not contained in the Galois group of the extension $\mathbb{Q}(E[2])/\mathbb{Q}(\sqrt{\mathrm{Disc}(E)})$. Now this last group has generically order 3, hence the condition is equivalent to say that $\rho(I_v)$ is not inside a group of order 3. So it is either a group of order 2 or 6, but the last could happen. (Jordan's comment in response: "Really sorry. The question I asked should be OK so long as the prime in question is not 2 or 3. A solution assuming the prime is 2 or 3 is a-OK.")
  - (OPTIONAL CHALLENGE EXERCISE) Suppose Δ is a perfect cube in K. What can we say about the image of the mod-3 Galois representation $\overline{\rho}_{E,3}$? Feel free to investigate this numerically using pari or MAGMA.

  (c) Suppose that $K = \mathbb{Q}$, and that $\#E(F_p)$ is even for all but finitely many primes p. Prove that $E[2]$ contains a nonzero point defined over $\mathbb{Q}$.
- Wedge product problems: If V is a vector space over a field k, we define the "wedge product" $\wedge^2 V$ to be the quotient of $V \otimes V$ by the subspace generated by all elements of the form $v \otimes v$, as v ranges over V. We denote the image of $v \otimes w$ in $\wedge^2 V$ by $v \wedge w$. (So, for instance, $v \wedge v = 0$.).
  (a) Suppose $\dim V = 2$. Show that $\dim \wedge^2 V = 1$.
  (b) Suppose that g is an automorphism of V, i.e. an element of $\mathrm{GL}(V)$. Then g induces an automorphism of $\wedge^2 V$ by the rule
  $$g(v \wedge w) = gv \wedge gw.$$
  This gives a homomorphism
  $$\mathrm{GL}(V) \to \mathrm{GL}(\wedge^2 V).$$
  Suppose $V = k^2$. Then $\wedge^2 V$ is 1-dimensional, so $\mathrm{GL}(\wedge^2 V)$ is canonically identified with $k^\times$. Prove that the resulting map $M_2(k) \to k^\times$ is the determinant.
  (c) Using the Weil pairing, prove that there exists a homomorphism $\wedge^2 E[p] \to \mu_p$ which is equivariant for the action of the Galois group on either side. Using this and (b), prove that the determinant of $\overline{\rho}_{E,p}$ is the cyclotomic character mod p.

- 5.3, 5.4, 5.6, 5.12, 6.7, 6.8, 6.9, 6.10 (note – for 6.8-10, you will definitely want to have read section VI.4 of Silverman, which is more explicit than I was about the lattice-theoretic description of isogenies of complex elliptic curves), 7.1, 7.5.
- (ISOGENIES OVER EXTENSION FIELDS) Let $E : y^2 = f(x)$ be the equation for an elliptic curve over a finite field $\mathbb{F}_q$, where $char(q) > 3$. Let d in $\mathbb{F}_q$ be a non quadratic residue, and write E_d for the elliptic curve $dy^2 = f(x)$. This is called a "quadratic twist" of E.
  (a) Show that E_d and E are isomorphic (whence isogenous) over $\mathbb{F}_{q^2}$. In particular, they have the same j-invariant.
  (b) Show that $a(E_d) = -a(E)$. In particular, by problem 5.4, E_d and E are isogenous over $\mathbb{F}_q$ if and only if $a(E) = 0$.

optional Now suppose $a(E) = 0$. Are E and E_d isomorphic over $\mathbb{F}_q$?

- (ZETA FUNCTIONS OF PRODUCTS) Let $A = E_1 \times E_2$ be the direct product of two elliptic curves. A is an example of an "abelian surface." By definition, $A(\mathbb{F}_q) = E_1(\mathbb{F}_q) \times E_2(\mathbb{F}_q)$. Prove that the Weil conjectures hold for A (given that you already know they hold for E_1 and E_2.)
- 7.8, 7.9, 8.3, 8.8, 8.15, 8.19 (8.19 is about L-functions and would be a good one to do in advance of Riad's talk.) OPTIONAL (but required for people who know or want to learn the notation of group cohomology) 8.5
- Diamond Shurman Problems: 1.1.3, 1.2.3, 1.2.5, 1.2.11, 1.5.2