ELLIPTIC CURVES, MODULAR CUVERS, AND MODULAR FORMS, WEEK 1

Definition 1. Let K be a field. An elliptic curve E/K is a smooth projective curve of genus 1 over K, together with a point $\mathcal{O} \in E(K)$.

We will prove that an an elliptic curve has an equation of the form

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

Theorem 1. *Every elliptic curve is the projective closure of an equation of the above form with* $\mathcal{O} = (0 : 1 : 0)$.

The a_i have weight i in the following sense. Make a change of variables $x \mapsto \lambda^2 x, y \mapsto \lambda^3 y$ changes a_i to $\lambda^{-i}a_i$.

$$\lambda^6y^2 + \lambda^5a_1xy + \lambda^3a_3y = \lambda^6x^3 + \lambda^4a_2x^2 + \lambda^2a_4x + a^6, \text{ dividing by } \lambda^6 \text{ gives}$$

$$y^2 + \lambda^{-1}a_1xy + \lambda^{-3}a_3y = x^3 + \lambda^{-2}a_2x^2 + \lambda^{-4}a_4x + a^6.$$

Proof. $E/K, \mathcal{O} \in E(K)$, genus $E = 1$. Let $L(n\mathcal{O})$ be the space of functions on E that is regular outside $\mathcal{O}$ and with a pole of order $\leq n$ at $\mathcal{O}$. Then $\dim(L(n\mathcal{O})) = l(n\mathcal{O}) = n$ for $n \geq 1$ by Riemann-Roch. Then we consider
$L(\mathcal{O}) = K$
$L(2\mathcal{O})$ contains $x \notin K$
$L(3\mathcal{O})$ contains $y \notin K \oplus Kx$
$L(4\mathcal{O})$ contains $1, x, y, x^2$, which are linearly independent (distinct orders) so they generate $L(4\mathcal{O})$
$L(5\mathcal{O})$ contains $1, x, y, x^2, xy$, again are linearly independent so they generate $L(5\mathcal{O})$
$L(6\mathcal{O})$ contains $1, x, y, x^2, xy, x^3, y^2$, but now are linearly dependent as $\dim(L(6\mathcal{O})) = 6$. Because of the linearly dependence we have an equation of the form:

$$cy^2 + a_1xy + a_3y = c'x^3 + a_2x^2 + a_4x + a_6.$$

We want to change x and y such that $c = c'$. We change $x \mapsto \alpha x$, $y \mapsto \beta y$. With that the coefficients of y^2 and x^3 become $c\beta^2, c'\alpha^3$ respectively. Since we want them equal, take $\alpha = \beta = c/c'$. Then with the new x, y we get $c = c'$. As $c \neq 0$, scaling by c we can have $c = 1$.

Since $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we get a map $\phi : E \to \mathbb{P}^2$ such that the product of the degree of the map $E \to \phi(E)$ with $\deg(\phi(E))$ is 3. But $\deg(\phi(E)) = 3$, so degree of the map $E \to \phi(E)$ is 1, which implies that ϕ is an isomorphism to its image. □

Remark. If x, y are other functions such that $x_1 \in L(2\mathcal{O})\backslash K, y_1 \in L(3\mathcal{O})\backslash L(2\mathcal{O})$ such that they satisfy $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. Then $x_1 = \alpha^2x+\beta, y_1 = \alpha^3y+\delta x+\epsilon$.

Suppose K has characteristic $\neq 2$. i Then by completing the square of the left side in $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, we get $\left(y + \frac{a_1x+a_3}{2}\right)^2 - \left(\frac{a_1x+a_3}{2}\right)^2 = x^3+a_2x^2+a_4x+a_6$. Then change $y \mapsto y - \frac{a_1x+a_3}{2}$ to have $y^2 = x^3 + b_2x^2 + b_4x + b_6$.

If characteristic of $K \neq 2, 3$, we can change x to $x - b_2/3$ and get an equation $y^2 = x^3 + c_4x + c_6$, where c_i are polynomails in a_j. Note that x, y are unique up to scalar of the form

$$x \mapsto \alpha^2 x, y \mapsto \alpha^3 y, c_4 \mapsto \alpha^{-4} c_4, c_6 \mapsto \alpha^{-6} c_6.$$

The equation is smooth iff $\Delta = 4c_4^3 + 27c_6^2 \neq 0$.

Definition 2. $j(E) = \frac{1728(4c_4)^3}{-16\Delta}$. $j(E)$ depends only on $E, \mathcal{O}$, not on the choice of x, y.

Definition 3. Two elliptic curve E, E' are isomorphic if $\exists$ an isomorphism of algebraic curves $\phi : E \to E'$ such that $\phi(\mathcal{O}) = \mathcal{O}'$.

Proposition 2. *For every $j \in K$, there exists an elliptic curve E/K such that $j(E) = j$.*

Proof. If $j \neq 0, 1728$, let $k = \frac{j}{1728-j}$ and $E : x^3 + 3kx + 2k$ to get $j(E) = j$. If $j = 0$, then $E : y^2 = x^3 + 1$ has $j(E) = 0$. If $j = 1728$, choose $E : y^2 = x^3 + x$. □

Theorem 3. *If E, E' are elliptic curves and $j(E) = j(E')$ then E and E' are isomorphic over $\bar{K}$.*

Proof. Let $E : y^2 = x^3 + c_4x + c_6, E' : y^2 = x^3 + c_4'x + c_6'$. Suppose $j(E) = j(E')$. If $c_4' \neq 0$, then $j(E) = j(E') \neq 0$, so $c_4 \neq 0$. By choosing an appropriate $\lambda = (\frac{c_4'}{c_4})^{(1/4)}$ we can assume $c_4 = c_4'$. Then we have

$$4c_4^3 + 27c_6^2 = \Delta = \Delta' = 4{c_4'}^3 + 27{c_6'}^2 \Rightarrow {c_6'}^2 = c_6^2.$$

If $c_6 = c_6'$, then $E = E'$. If $c_6 = -c_6'$, then $y^2 = x^3 + c_4x + c_6, y^2 = x^3 + c_4x - c_6$. By sending $x \mapsto -x, y \mapsto iy$ give us the isomorphism.

If $c_4' = 0$, then $c_4 = 0$. Thus $y^2 = x^3 + c_6, y^2 = x^3 + c_6'$. Choose $\lambda = (\frac{c_6'}{c_6})^{1/6}$. □

Note: $y^2 = x^3 + 1$ has $j = 0$. There is a bijection between K isomorphism classes of elliptic curves E/K with $j = 0$ and $K^\times/(K^\times)^6$. For $j = 1728$, $E : y^2 = x^3 + c_4x$ there is the bijection of the K isomorphism classes to $K^\times/(K^\times)^4$. For $j \neq 0, 1728, y^2 = x^3 + c_4x + c_6, dy^2 = x^3 + c_4x + c_6$. The second equation is the same as $y^2 = x^3 + d^2c_4x + d^3c_6$. Then the set of isomorphism classes corresponds to $K^\times/(K^\times)^2$.

Definition 4. Suppose $\mathcal{X}$ is a class of algebraic varieties over K, algebraically closed. An algebraic variety X/k is a coarse moduli space for $\mathcal{X}$ if
a) $\mathcal{X}$/isomorphism is in bijection with $X(k)$.
b) $\forall Y, T$, and $f : Y \to T$, flat map of algebraic varieties over k such that $f^{-1}(t) \in \mathcal{X}, \forall t \in T(k)$, then $\exists$ morphism $j : T \to X$ such that the isomorphism class of $f^{-1}(t)$ corresponds to $j(t)$ under the bijection of a).

Definition 5. X is a fine moduli space for $\mathcal{X}$ if moreover $\exists f_0 : Y_0 \to X$ flat family such that $f_0^{-1}(x) \in \mathcal{X}, \forall x \in X(k), f : Y \to T$ as in b), f is the pullback of f_0 by j.

Corollary 4. *$\mathbb{A}^1$ is a coarse moduli space for elliptic curves.*

$\mathbb{A}^1(k)$ is in bijection with elliptic curves over k/isomorphism. Suppose Y, T are algebraic varieties over k and $f : Y \to T$ is flat, and $s : T \to Y, f(s(t)) = t$ such that $E = f^{-1}(t)$ with $\mathcal{O} = s(t)$ is an elliptic curve. Then the map j in the definition is the j-invariant of the generic fiber of f, which is a function in $K(T)$.

Example: $y^2 = x^3 + 3tx + 2t, t \neq 0 \subset \mathbb{P}^2 \times \mathbb{A}^1 - \{0, -1\}$, $Y \to T = \mathbb{A}^1 - \{0, -1\}$ with coordinate t. Then direct computation yields $\Delta = 4(3t)^3 + 27(2t)^2 = 3^3 2^2 t^2 (t + 1)$, and $j = \frac{4 \cdot 1728 \cdot 3^3 t^3}{3^3 2^2 t^2 (t+1)} = 1728t/(t + 1)$.

We need to give $j_0 : T \to \mathbb{A}^1$ such that $j(f^{-1}(t)) = j_0(t)$. The generic fiber of f is an elliptic curve over $k(T)$, so it has a j invariant $j \in k(T)$ so a regular map $j_0 : T \to \mathbb{A}^1$. $y^2 = x^3 + c_4x + c_6$, $\frac{*c_4^4}{\Delta}$.
There is no fine moduli space for elliptic curves but we will construct fine moduli spaces for elliptic curves with additional structure.

1 The Group Law on an Elliptic Curve

January 26, 2010

We assume temporarily that K is algebraically closed. We fix a smooth projective curve C/k. A *divisor* on C is a formal linear combination of the points of C with coefficients in $\mathbb{Z}$. We denote the collection of divisors on C by $\mathrm{Div}(C)$. That is,

$$\mathrm{Div}(C) = \{\textstyle\sum_{P\in C} n_P P | n_P \in \mathbb{Z} \text{ all but finitely-many zero}\}.$$

We give $\mathrm{Div}(C)$ the obvious addition and so it becomes an abelian group (the free abelian group on the points of C).

The *degree* of a divisor is defined to be the sum of its coefficients and the subgroup of divisors of degree zero is denoted $\mathrm{Div}^0(C)$. If $f \in K(C)^\times$, the divisor of f is defined to be $(f) = \sum_{P\in C} \mathrm{ord}_P(f)P$. A divisor which comes from a function in this way is called *principal* and the collection of principal divisors is denoted $\mathrm{Prin}(C)$. Since a function on C has the same number of zeros as it has poles (counted with multiplicity) we have $\mathrm{Prin}(C) \subset \mathrm{Div}^0(C)$. Likewise, the relation $(fg) = (f) + (g)$ shows that $\mathrm{Prin}(C)$ is a subgroup of $\mathrm{Div}(C)$.

The *Jacobian* of C is the quotient group

$$\mathrm{Jac}(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C).$$

We say that two divisors are *linearly equivalent* if the differ by a principal divisor. In particular, two divisors of degree zero are linearly equivalent if and only if they are equal in the Jacobian. In the case of an elliptic curve, we get a very nice interpretation of the Jacobian.

Theorem. *If E is an elliptic curve, the map $E \to \mathrm{Jac}(E)$ defined by $P \mapsto [P - \mathcal{O}]$ is a bijection (here the brackets of course denote the equivalence class of $P - \mathcal{O}$ in $\mathrm{Jac}(E)$; $\mathcal{O}$ is the distinguished point of E).*

Proof. We first show surjectivity. If D is a divisor on E of degree zero, then the divisor $D + \mathcal{O}$ has degree 1. Hence, by the Riemann-Roch Theorem, we have $\ell(D + \mathcal{O}) = 1$. Thus we may find an $f \in L(D + \mathcal{O}) - \{0\}$. By definition then, every coefficient of $(f) + D + \mathcal{O}$ is nonnegative. On the other hand, the degree of $(f) + D + \mathcal{O}$ is one. We conclude that $(f) + D + \mathcal{O} = P$ for some $P \in C$. That is, $D + (f) = P - \mathcal{O}$ which is to say that $[D] = [P - \mathcal{O}]$. Hence our map is surjective.

Next suppose that for $P, Q \in E$, $[P - \mathcal{O}] = [Q - \mathcal{O}]$. Then $P - \mathcal{O}$ and $Q - \mathcal{O}$ differ by a principal divisor which is to say that P and Q differ by a principal divisor. Thus we have some $f \in K(E)^\times$ with $(f) = P - Q$. If P is not equal to Q, we see that f has a simple zero at P, a simple pole at Q, and no other poles or zeros. In other words, f gives a function $E \to \mathbb{P}^1$ of degree 1. We conclude that E is isomorphic to $\mathbb{P}^1$. This is a contradiction since E has genus one and $\mathbb{P}^1$ has genus zero. Thus $P = Q$ and our map is injective. □

This theorem gives us an identification of E with $\mathrm{Jac}(E)$ as sets. In particular, we may use the group operation on $\mathrm{Jac}(E)$ to get a group operation on E. This group operation is defined by saying that $P+Q=R$ if and only $[P+Q]=[R+\mathcal{O}]$ (P,Q,R of course being points of E).

Recall that we may fix an embedding $E \hookrightarrow \mathbb{P}^2$ whose image is a cubic in $\mathbb{P}^2$. Via this embedding, we get a geometric interpretation of the group law on E.

Proposition. *For points $P,Q,R \in E$, we have $P+Q+R=\mathcal{O}$ if and only if P, Q, and R are collinear in $\mathbb{P}^2$.*

Proof. To say $P+Q+R=\mathcal{O}$ is the same as saying that $[P+Q+R-3\mathcal{O}]=0$, which is the same saying that $P+Q+R-3\mathcal{O}=(f)$ for some $f \in K(E)^\times$. Now such an f would, by definition, lie in $L(3\mathcal{O})$ (I think that we do not need to assume that P, Q, and R are not equal to $\mathcal{O}$; If say $R=\mathcal{O}$, the divisor in question would be $P+Q-2\mathcal{O}$ which would still lie in $L(3\mathcal{O})$; it would of course also lie in $L(2\mathcal{O})$; i.e., we would get $\gamma=0$ in the notation below). Our embedding was constructed by choosing x and y such that $\{1,x,y\}$ is a basis for $L(3\mathcal{O})$. $P+Q+R=\mathcal{O}$ is equivalent to having a relation of the form $P+Q+R-3\mathcal{O}=(\alpha+\beta x+\gamma y)$ for some $\alpha,\beta,\gamma \in K$, i.e. to P, Q, and R being collinear (and lying on the line $\alpha+\beta x+\gamma y=0$). □

This last observation allows us to write down the group law explicitly. Suppose that our embedding corresponds to the equation

$$y^2=x^3+c_4x+c_6.$$

Let $P=(x_1,y_1)$ and $Q=(x_2,y_2)$. We will assume that $x_1 \neq x_2$ (the case $x_1=x_2$ may be calculated in a similar fashion). Define $R=(x_3,y_3)$ by $P+Q=R$ (by assuming R has this form, we are assuming that $P+Q \neq \mathcal{O}$, i.e., that P and Q are not inverses). First consider the function $x-x_3$. Since (x_3,y_3) is a solution of the equation above, $(x_3,-y_3)$ is as well. Thus $x-x_3$ has zeros at $(x_3,\pm y_3)$. Since $x-x_3 \in L(2\mathcal{O})$, we conclude that the divisor of $x-x_3$ is $(x_3,y_3)+(x_3,-y_3)-2\mathcal{O}$. But that implies that $(x_3,y_3)+(x_3,-y_3)=\mathcal{O}$ so that $-(x_3,y_3)=(x_3,-y_3)$.

Now since $P+Q=R$, we have $P+Q+(-R)=\mathcal{O}$ which implies that P, Q, and $-R$ are collinear. The line through P and Q is of course defined by $y=m(x-x_1)+y_1$, where $m=(y_2-y_1)/(x_2-x_1)$. Thus P, Q, and $-R$ must be the points of intersection of E and this line. Thus x_1, x_2, and x_3 must be the solutions to

$$(m(x-x_1)+y_1)^2=x^3+c_4x+c_6,$$

a monic cubic equation. In particular, $x_1+x_2+x_3$ is the coefficient of the x^2 term which is m^2. We conclude that

$$x_3=-x_1-x_2+\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 \text{ and } y_3=-\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_3-x_1)-y_1.$$

The form of these equations (and those which correspond to the other cases) gives us an important observation about the group law on E, but first we give a definition. At this point, we drop the assumption that K is algebraically closed.

Definition. An *algebraic group* over K is an algebraic set G/K, together with a point $e \in G(K)$, and morphisms $\text{inv} : G \to G$ and $\mu : G \times G \to G$ which satisfy the following conditions

1. (associativity) the diagram

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\text{id}_G \times \mu} & G \times G \\ \downarrow{\scriptstyle \mu \times \text{id}_G} & & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow{\mu} & G \end{array}$$

   commutes,

2. (left and right identity) the maps $G \to G$ given by $x \mapsto \mu(e, x)$ and $x \mapsto \mu(x, e)$ are both equal to id_G, and

3. (left and right inverse) the compositions

$$G \xrightarrow{\text{inv} \times \text{id}_G} G \times G \xrightarrow{\mu} G \text{ and } G \xrightarrow{\text{id}_G \times \text{inv}} G \times G \xrightarrow{\mu} G$$

   are both equal to the constant map $x \mapsto e$.

We remark that the definition of a algebraic group is essentially a reformulation of the definition of a group except that we require the underlying set of our group to have the structure of an algebraic set and we require the multiplication and inversion maps to be morphisms. Since our expressions for the group law on E were rational functions in the coordinates of P and Q, we conclude the following.

Corollary. *E is an algebraic group.*

We also point out that though we used an algebraically closed field to define the group law on E, $E(K)$ is a subgroup of $E(\bar{K})$, since the expressions above for multiplication and inversion did not force us to work outside of K.

We give a few examples of other group schemes. We have the algebraic set $\mathbb{A}^1 - \{0\}$ (which may of course be seen to be an algebraic set by identifying it with the solution set to $xy = 1$ inside of $\mathbb{A}^2$ in the usual way). Defining $\mu(x, y) = xy$ makes $\mathbb{A}^1 - \{0\}$ into an algebraic group denoted $\mathbb{G}_m$ (the subscript m standing for 'multiplication').

The set $\mu_n = \{x \in \mathbb{G}_m | x^n = 1\}$ is a algebraic subgroup (in the obvious sense) of $\mathbb{G}_m$. If K is algebraic closed and its characteristic does not divide n, then μ_n is isomorphic as a group to $\mathbb{Z}/n\mathbb{Z}$. Of course for fields that are not algebraically closed, this need not be the case. If $n = p$ is the characteristic of p, μ_n has only a single point.

As with the example just discussed, the torsion points of an elliptic curve are also very important. For a natural number n, we denote the n-torsion subgroup of E by $E[n]$.

We consider the case $n = 2$. Suppose that E is given by the equation $y^2 = x^3 + ax + b$. We see that $P \in E[2]$ if and only if $2P - 2\mathcal{O} = (f)$ for some $f \in K(E)^\times$. As above (when we showed that three points sum to zero if and only if they are collinear), f must have the form $f = x - \beta$ (here we are assuming that $P \neq \mathcal{O}$ and proceeding, without loss of generality, by scaling f).

Now a point on E is a zero of f if and only if it has the form (β, y) with $y^2 = \beta^2 + a\beta + b$. Hence, since f has only the single zero P, we conclude that $\beta^2 + a\beta + b = 0$ and that $P = (\beta, 0)$. Thus

$$E[2] = \{\mathcal{O}\} \cup \{(\beta, 0) | \beta^2 + a\beta + b = 0\}.$$

In particular, we have at most 4 points in $E[2]$ and so $E[2]$ is either trivial as a group or isomorphic to $\mathbb{Z}/2$ of $(\mathbb{Z}/2\mathbb{Z})^2$, depending on the number of roots of $x^3 + ax + b$ lying in K. We note that this polynomial is always separable since E is smooth and so the order of $E[2]$ over $\bar{K}$ is always 4.

We also remark that we assumed in the previous discussion that E had the form $y^2 = x^3 + ax + b$, an assumption that only holds in general for characteristics other than 2 and 3. For characteristic 3, E still has the form $y^2 = f(x)$ where $f(x)$ is a cubic polynomial and the same argument goes through. In characteristic 2, however, $E[2]$ has either order 1 or order 2, never order 4.

If $\#E[2] = 4$, then E has the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$. A change of variables can then be made to put E in the form $y^2 = x(x - 1)(x - \lambda)$ (this is of course not a Weierstrauss equation: it has a nonzero x^2 term, it is known as the Legendre equation).

2 Isogenies and the map $[n]$

January 28, 2010

Before we continue to study elliptic curves, we give some general results about algebraic groups to demonstrate the general context of our observations.

Proposition. *A reduced algebraic group G is always smooth as a variety.*

Proof. We use the general fact that a reduced algebraic set always has a smooth point (essentially a point which is not smooth must satisfy equations based on the Jacobian matrix and so having a point is a degenerate condition). Let then $P_0 \in G$ be a smooth point and suppose that $P \in G$ is any point. Then the map $G \to G$ given by left translation PP_0^{-1} is an isomorphism of varieties (its inverse being left translation by P_0P^{-1}). Furthermore it takes the smooth point P_0 to the point P and we conclude that P is smooth. □

We conclude that every function and map on a reduced algebraic group can be described locally by a power series. In particular, we may apply this observation to the multiplication map $\mu : G \times G \to G$. Thus if G is dimension n then locally near the identity e, we have

$$\mu(X_1, \ldots, X_n, Y_1, \ldots, Y_n) = (\mu_1, \ldots, \mu_n)$$

with $\mu_i \in k[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]]$. The fact that $\mu(e, e) = e$ then translates to $\mu_i(0, \ldots, 0) = 0$. Likewise the facts that $\mu(P, e) = 0$ and $\mu(e, Q) = 0$ mean that $\mu_i(X_1, \ldots, X_n, 0, \ldots, 0) = X_i$ and $\mu_i(0, \ldots, 0, Y_1, \ldots, Y_n) = Y_i$ respectively. We conclude that μ_i has the form $X_i + Y_i$ plus terms of higher order.

In the case of an elliptic curve, the dimension is one and so our map is described locally by $\mu(X, Y) = X + Y + \ldots$. If the curve is given by $y^2 = x^3 + ax + b$, x has a pole of order 2 at $\mathcal{O}$ and y has a pole of order 3. Hence $t = x/y$ has a zero of order 1 and so is a local parameter at $\mathcal{O}$. Moreover, we see that $x = 1/t^2 + \ldots$ and $y = 1/t^3 + \ldots$. We also remark that the change of coordinates $x \mapsto \alpha^2 x$ and $y \mapsto \alpha^3 y$ takes t to $(1/\alpha)t$. Thus fixing a parameter at $\mathcal{O}$ is essentially the same a choosing an equation for E of the type above. We also point out that our previous explicit formulation of the group law may be used to determine $\mu(X, Y)$.

In general, a power series $\mu \in k[[X, Y]]$ such that $\mu(X, 0) = X$, $\mu(0, Y) = Y$, and $\mu(X, \mu(Y, Z)) = \mu(\mu(X, Y), Z)$ is called a *formal group law* (in one variable). The conditions given are of course analogous to zero being the identity for the group and the associativity property. It turns out that the condition analogous to the existence of inverses is a consequence of the conditions are already given and so it is not necessary to put this requirement on a formal group.

We define the map $[n] : E \to E$ to be the morphism on E given my multiplication by n, that is, it is given by $P \mapsto nP$. $[0]$ is of course the constant map $P \mapsto \mathcal{O}$.

Proposition. *The map $[n]$ is nonconstant for $n \neq 0$. If the characteristic of K is zero or does not divide n, the map is also separable.*

Proof. We compute the derivative of the map at $\mathcal{O}$. Indeed, locally we have $\mu(X, Y) = X + Y + \ldots$. In particular, $[2](X) = 2X + \ldots$. Thus $[3](X) = (X, [2](X)) = 3X + \ldots$. In this way (using induction to be strict), we conclude that $[n](X) = nX + \ldots$. Thus the derivative of $[n]$ at $\mathcal{O}$ is n (i.e., corresponds to multiplication by n on the tangent space to E at $\mathcal{O}$). Hence if the characteristic of K does not divide n (or if it is zero), we see that the derivative in question is nonzero. This implies that the map is nonconstant and separable.

We thus reduce to the case that $n = p^r s$, p being the (positive) characteristic of K. If E is given by $y^2 = f(x)$, we have seen that the point $(\beta, 0)$ is a point on E of order 2 if $f(\beta) = 0$. Hence if $p \neq 2$, we may find a point P of order 2 on E. Since p is odd, this implies that $[p]P = P$. Since $[p]\mathcal{O} = \mathcal{O} \neq P$, we conclude that $[p]$ is non constant. But then

$$[n] = \underbrace{[p] \circ \cdots \circ [p]}_{\text{r times}} \circ [s]$$

is a composition of nonconstant maps and so is itself nonconstant. For the case $p = 2$, one need only check directly that the map $[2]$ is nonconstant and then apply the same argument. □

We remark that $E[n] = [n]^{-1}(\mathcal{O})$. Now, since $[n] : E \to E$ is a nonconstant map of curves (for $n \neq 0$), we are led to find its degree. For the separable case,

it is natural to apply Hurwitz's Formula. We recall that this formula states that if $f : C' \to C$ is nonconstant map of curves then we have

$$2g' - 2 = (\deg f)(2g - 2) + r$$

if g' and g are the genera of C' and C respectively and r is the ramification. Unfortunately in the case of a map between elliptic curves we have $g = g' = 1$ and so we can conclude only that $r = 0$ (a fact that is easy to see since translation preserves ramification index). In particular, this strategy provides no information about the degree of $[n]$. In fact, we will compute the degree of $[n]$, but the proof will require more work.

Since our notion of an elliptic curve carries with it not just a smooth curve of genus one but also a distinguished point, it is natural to consider those maps which preserve the distinguished points. This leads to the following definition.

Definition. A nonconstant map $f : E \to E'$ between elliptic curves is called an *isogeny* if it satisfies $f(\mathcal{O}) = \mathcal{O}'$, where $\mathcal{O}$ and $\mathcal{O}'$ are the distinguished points of E and E' respectively. We say that two elliptic curves are *isogenous* if there is an isogeny between them.

Of course the map $[n] : E \to E$ is an isogeny. We remark that the terminology isogenous does not reflect the direction of an isogeny between E and E'. This apparent oversight is justified by the following theorem.

Theorem. *If $f : E \to E'$ is an isogeny and $\deg f = n$, then there exists an isogeny $f' : E' \to E$ of degree n such that*

1. *$f \circ f' = [n]$ on E' and*
2. *$f' \circ f = [n]$ on E.*

In particular, since every nonconstant map curves is finite, the existence of an isogeny $E \to E'$ implies the existence of an isogeny in the opposite direction. We will prove this last theorem, but first we prove the following.

Theorem. *Every isogeny is a group homomorphism.*

Proof. Suppose that $f : E \to E'$ is an isogeny. Then we have the homomorphism $f_* : \mathrm{Div}(E) \to \mathrm{Div}(E')$ given by $f_*(\sum_P n_P P) = \sum_P n_P f(P)$. Moreover, since f_* certainly respects the degree of a divisor, it restricts to a map $\mathrm{Div}^0(E) \to \mathrm{Div}^0(E')$. We will show that it further induces a homomorphism $\mathrm{Jac}(E) \to \mathrm{Jac}(E')$.

For this, we need to show that $f_*(\mathrm{Prin}(E)) \subset \mathrm{Prin}(E')$. Well, we have the map $K(E') \to K(E)$ (that is, a function on E' may be pre-composed with f to give a function on E). Since f is a map of curves, this map makes $K(E)$ into a finite extension of $K(E')$. Thus we may consider the norm map $K(E) \to K(E')$. We state as a fact the equality $f_*((x)) = (\mathrm{Norm}(x))$ for $x \in K(E)$. We remark that this equality translates to the fact that $f^{-1}(P)$ has $\deg f$ points, counted with multiplicity. We conclude that $f_*(\mathrm{Prin}(E)) \subset \mathrm{Prin}(E')$.

But now we have the induced map $\mathrm{Jac}(E) \to \mathrm{Jac}(E')$. By definition, it takes $P - \mathcal{O}$ to $f(P) - f(\mathcal{O}) = f(P) - \mathcal{O}'$. But under the identification $E = \mathrm{Jac}(E)$ and $E' = \mathrm{Jac}(E')$, this is to say that the induced map is the same as $f : E \to E'$ (we are of course neglecting the notation of equivalence classes to avoid confusion with the notation $[n]$). Since the induced map is a homomorphism by construction, we conclude that f is a homomorphism. □

We now prove the other theorem by a similar strategy. Indeed our proof was basically an analysis of the push-forward f_*. The proof of the other theorem will be an analysis of the pull-back f^*.

Proof. We define $f^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$ by $f^*(P) = \sum_{f(Q)=P} e_Q Q$, (where the E_Q are ramification indices) and extend linearly. Again since the ramification indices of points above P sum to $\deg(f)$, we conclude that f^* restricts to $\mathrm{Div}^0(E') \to \mathrm{Div}^0(E)$. Furthermore, $f^*((x)) = (x \circ f)$ and so f^* induces a map $\mathrm{Jac}(E') \to \mathrm{Jac}(E)$. Taking the corresponding map $E' \to E$ gives our definition of f'.

We check that $f' \circ f$ is multiplication by n. By definition,

$$f'(f(P)) = f^*(f(P) - \mathcal{O}') = \sum_{f(Q)=f(P)} e_Q Q - \sum_{f(Q)=\mathcal{O}'} e_Q Q.$$

Now, since f is a homomorphism, $f(Q) = \mathcal{O}$ is equivalent to $f(Q+P) = f(P)$. Thus, translation by P provides a bijection between the pre-image of $f(P)$ and that of $\mathcal{O}'$ and so we conclude that the expression above is

$$\sum_{f(Q)=\mathcal{O}'} e_{Q+P}(Q+P) - e_Q Q$$

(the expression $Q + P$ in parenthesis of course reflects the operation on E and not on $\mathrm{Jac}(E)$, but, as we will use momentarily, these operations are the same in the obvious sense and so we do not distinguish between them). Since translation preserves ramification, we have $e_{Q+P} = e_Q$. Thus the expression in question is

$$\sum_{f(Q)=0} e_Q(Q + P - Q) = \sum_{f(Q)=0} e_Q P = (\deg f)P,$$

as claimed. The other requirement is of course the same proof. □

ELLIPTIC CURVES
WEEK 3

2-2-10

First, we recall what we covered last time about isogenies.

Definition 1. An isogeny is a (nonconstant) map $f : E \to E'$ between elliptic curves such that $f(\mathcal{O}) = \mathcal{O}'$.

Ex: $[n] : E \to E$, $P \mapsto nP$.

Theorem 2. *An isogeny is a homomorphism.*

Theorem 3. *Given a nonconstant isogeny $f : E \to E'$, $n = \deg f$, there exists a unique $f' : E' \to E$ (sometimes denoted by f^* or $\hat{f}$) such that*

$$f \circ f' = [n] \quad \text{on } E', \text{ and}$$
$$f' \circ f = [n] \quad \text{on } E$$

Our goal is to prove the following theorem:

Theorem 4. $\deg[n] = n^2$

This follows from the following theorem:

Theorem 5. $[n]' = [n]$

Claim 6. Theorem 5 implies Theorem 4

Proof. By the definition of the dual of an isogeny in Theorem 3, $[n]' \circ [n] = [\deg[n]]$. If $[n]' = [n]$, we have

$$[n]' \circ [n] = [n] \circ [n] = [n^2] = [\deg[n]]$$

We know that $n \mapsto [n]$ is an injective map of $\mathbb{Z} \to End(E)$. This is because if $n \neq 0$, then $[n] \neq 0$, and we know that $n \mapsto [n]$ is a homomorphism ($[n+m](P) = (n+m)P = nP + mP = [n](P) + [n](P)$). Hence, $[n^2] = [\deg[n]]$ implies that $n^2 = \deg[n]$, as desired. □

We can prove Theorem 5 using the following lemma:

Lemma 7. *If $f, g : E \to E'$ are isogenies, then $(f+g)' = f' + g'$.*

Claim 8. Lemma 7 implies Theorem 5

Proof. We prove the claim (for positive n) by induction on n. For the base case, we have $\deg[1] = 1$, so by Theorem 3, $[1]' \circ [1] = [1]$. Since $[1]$ is the identity, this imples $[1]' = [1]$.

For $n+1$, the lemma says that

$$\begin{aligned}[n+1]' = ([n]+[1])' &= [n]' + [1]' \\ &= [n] + [1] \quad \text{by the inductive step} \\ &= [n+1] \quad \text{by the lemma again}\end{aligned}$$

For negative n, we have $[-1] \circ [-1] = [1] = [\deg[-1]]$, so the uniqueness in Theorem 3 tells us that $[-1]' = [-1]$. The inductive step on $[n-1]$ is similar to the one above. □

Finally, we prove Lemma 7.

Proof. (This proof works for $f \neq -g$). Let $f : E \to E'$ be an isogeny. We have seen that $f'(P)$ is the pull-back $f^*(P) = \sum_{f(Q)=P} e_Q Q$.

Define $E : y^2 = x^3 + ax + b$ and $E' : (y')^2 = (x')^3 + a'x' + b'$. We have

$$f(x, y) = (R(x, y), S(x, y))$$

for some $R(x, y), S(x, y) \in K(x, y) = K(E) = F$. Let $P_{gen} = (x, y) \in E(F)$ be the generic point, and $f(P_{gen}) = (R, S)$. As elements of F, (R, S) satisfies the equation of E', so $(R, S) \in E'(F)$.

By definition, we have

$$f(P_{gen}) + g(P_{gen}) = (f + g)(P_{gen})$$

So then by the definition of addition in E', we have

$$f(P_{gen}) + g(P_{gen}) - ((f + g)(P_{gen}) - \mathcal{O}) \sim 0$$

meaning that it is the divisor of some function $z \in F(E') = F(x', y')$ ($\sim$ denotes linear equivalence of divisors). We see from the divisor that z has zeroes at $f(P_{gen})$ and $g(P_{gen})$, and poles at $(f + g)(P_{gen})$ and $\mathcal{O}$.

We can view z as a function on $E \times E'$, because $z \in F(x', y')$ implies that $z = \frac{u(x',y')}{v(x',y')}$, where $u(x', y'), v(x', y') \in F[x', y']$. That is, the coefficients of u and v are rational functions in x and y with coefficients in K. We now consider the divisor of z as a function on $E \times E'$.

Since z is zero at $f(P_{gen})$ when considered as a function on E', we see that z is zero on the graph of f when considered as a function on $E \times E'$. Similarly, z is zero on the graph of g, and z is infinite on the graph of the constant $\mathcal{O}$ and on the graph of $f+g$. z may also have zeroes or poles for some vertical lines over a divisor D_0 on E (that is, for $d_0 \times E'$ for certain $d_0 \in E$). So for all P, we have

$$(z(P)) = f^*(P) + g^*(P) - (f + g)^*(P) - \mathcal{O} + D_0$$

Hence,

$$f^*(P) + g^*(P) - (f + g)^*(P) - \mathcal{O} + D_0 \sim 0$$

Now D_0 has degree 0 and it is independent of P. Making $P = \mathcal{O}'$, we get

$$f^*(\mathcal{O}') + g^*(\mathcal{O}') - (f + g)^*(\mathcal{O}') - \mathcal{O} + D_0$$

So $D_0 \sim 0$. So for all P, we have

$$f'(P) + g'(P) - (f + g)'(P) - \mathcal{O} \sim 0$$

So $(f + g)'(P) = f'(P) + g'(P)$ for all P by our definition of addition in E. Hence, $(f + g)' = f' + g'$, as desired. □

Exercise 9. Complete the above proof for the case $g = -f$. That is, prove that $(-f)' = -f'$.

So $\deg[n] = n^2$, as claimed. There also exists an analytic proof of this (Exercise 3.8 in Silverman), as well as the computational proof outlined in Exercise 3.7 on pg 105 of Silverman's book.

2-4-10

Let E/K be an elliptic curve.

Proposition 10. *Suppose G is a finite subgroup of E. Then there exists an elliptic curve E'/K and an isogeny $f : E \to E'$ with kernel G (and deg $f = |G|$).*

Note: We will assume that K is algebraically closed ($K = \overline{K}$). If K is not algebraically closed, then E' is defined over K iff G is invariant under $\mathrm{Gal}(\overline{K}/K)$.

Proof. G acts on the curve E, by translation. That is, $\tau_{P_0} : E \to E$, $P \mapsto P + P_0$. τ_{P_0} is a rational map, so τ_{P_0} acts on $K(E)$ by $z \mapsto z \circ \tau_{P_0}$.

$K(E)^G$ is a subfield of $K(E)$, and $[K(E) : K(E)^G] = |G|$. Also, $K \subset K(E)^G$, and $K(E)^G/K$ is a function field in 1 variable. So $K(E)^G = K(C)$ for some smooth curve C/K, and we have a map $f : E \to C$. G acts without fixed points, so f is unramified. So by the Hurwitz theorem, C has genus 1. Now, $f(\mathcal{O}) \in C$ is a point, so $E' = (C, f(\mathcal{O}))$ is an elliptic curve, and $f : E \to E'$ is the desired isogeny. □

Exercise: Let $E : y^2 = x^3 + ax^2 + bx$. Compute $E/\langle(0,0)\rangle$.

Suppose $\mathrm{Char}(K) = 0$ or $\mathrm{Char}(K) = p$ where p does not divide n: $\#E[n] = n^2$, so $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$. Let $G \triangleleft E$ be finite (with p not dividing $|G|$ if $p > 0$). Then $G \triangleleft E[n]$ for some n (choose the minimal such n). We have $G \cong \mathbb{Z}/m \oplus \mathbb{Z}/m$ for some $m|n$, and this contains $H \cong \mathbb{Z}/m \oplus \mathbb{Z}/m$. We have the following sequence:

$$E \to E/H \to E/G$$

where the first map is $[m]$, $E/H \cong E$, and $E/G \cong E/(G/H)$. G/H is cyclic of order n/m.

Now suppose $\mathrm{Char}(k) > 0$, and we will consider the case where $p|n$. Define

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E^{(p)} : y^2 + a_1^p xy + a_3^p y = x^3 + a_2^p x^2 + a_4^p x + a_6^p$$

Let $F : E \to E^{(p)}$ be the Frobenius map $(x, y) \mapsto (x^p, y^p)$. This is an isogeny of degree p. F is purely inseparable, and $\ker(F)$ as a set is just $\{\mathcal{O}\}$.

F has a dual $F' : E^{(p)} \to E$. The map $V = F' : E^{(p)} \to E$ is called the Verschiebung (German for shift). We have $V \circ F = [p]$, and $\deg[p] = p^2$, so $\deg(V) = p$. Note that $E[p]$ is isomorphic as a group to $\ker(V)$. We have

$$\#\ker(V) = \begin{cases} 1 & \text{if } V \text{ is inseparable} \\ p & \text{if } V \text{ is separable} \end{cases}$$

The case where $\#\ker(V) = p$ is called the ordinary case. Here, $\#\ker[p^n] = p^n$.

The case where $\#\ker(V) = 1$ is called the supersingular case. Here, $\#\ker[p^n] = 1$.

Exercise: If $p = 2$, show that E is ordinary iff $a_1 \neq 0$ (figure out the point of order 2). If E is supersingular, then $j(E) = 0$, and E is isogenous over $\bar{k}$ to $y^2 + y = x^3$.

Now for $p > 2$, we have

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$
$$E^{(p)} : y^2 = x^3 + a_2^px^2 + a_4^px + a_6^p$$

So

$$(x^3 + a_2x^2 + a_4x + a_6)^{(p-1)/2} = U(x) + Ax^{p-1} + x^pW(x)$$

where $U(x)$ is a polynomial of degree $\leq p - 2$, $W(x)$ is a polynomial of degree $\frac{3(p-1)}{2} - p$, and A is the "Hasse invariant."

Theorem 11. *E is ordinary iff $A \neq 0$*

Proof. We only prove the "if" part. Suppose $A \neq 0$. Consider

$$C : \begin{cases} y^2 = x^3 + a_2x^2 + a_4x + a_6 \\ z^p - Az = yW(x) \end{cases}$$

We have a map $C \to E$, $(x, y, z) \mapsto (x, y)$. Since $\frac{d}{dz}[z^p - Az - yW(x)] = -A \neq 0$, this polynomial is separable (it has p distinct roots). V is clearly unramified away from $V^{-1}(\mathcal{O})$.

On E, $y^p = yU(x) + yAx^{p-1} + yx^pW(x)$. Dividing by x^p, we have

$$\left(\frac{y}{x}\right)^p - A\left(\frac{y}{x}\right) = yW(x) + \frac{yU(x)}{x^p}$$

Note that the last term $yU(X)/x^p$ has a zero at $\mathcal{O}$.

We can combine $z^p - Az = yW(x)$ with the above equation to get

$$(z - y/x)^p - A(z - y/x) = yU(x)/x^p$$

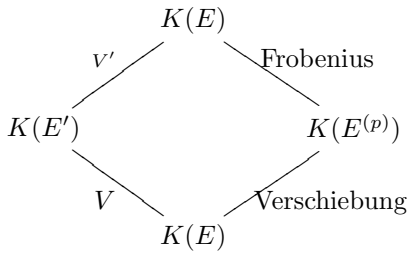
This is a local equation for $V : C \to E$ near $\mathcal{O}$, and it shows that it is unramified at $\mathcal{O}$.

Now, z has a simple pole at every $P \in V^{-1}(\mathcal{O})$. So

$$z = y/x + \alpha + \ldots, \alpha^p - A\alpha = 0$$

This proves that $V : C \to E$ is unramified. So C has genus 1, by the Hurwitz formula. Also, C has a rational point $\mathcal{O}'$ in $V^{-1}(\mathcal{O})$ corresponding to $\alpha = 0$. So $(C, \mathcal{O}')$ is an elliptic curve, E'.

The map $V : E' \to E$ is a separable isogeny of degree p. So $K(E)/K(E)$, via $V' \circ V = [p]$, is not purely inseparable, so the Verschiebung is separable and E is ordinary. See the following diagram of fields:



□

If K is algebraically closed, E has an equation $y^2 = x(x-1)(x-\lambda)$. We have

$$[x(x-1)(x-\lambda)]^{(p-1)/2} = x^{(p-1)/2} \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j} x^j (-1)^{[(p-1)/2]-j} \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k} x^k (-\lambda)^{[(p-1)/2]-k}$$

Now,

$$\begin{aligned} A(\lambda) &= \sum_{\substack{j=0 \\ j+k=\frac{p-1}{2}}}^{(p-1)/2} (-1)^{(p-1)/2} \binom{(p-1)/2}{j} (-\lambda)^{[(p-1)/2-k]} \binom{(p-1)/2}{k} \\ &= (-1)^{(p-1)/2} \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j}^2 \lambda^j \end{aligned}$$

Since $A(\lambda)$ is not identically equal to 0, there are only finitely many solutions to $A(\lambda) = 0$, and so only finitely many supersingular curves in $\mathrm{char}(p)$.

Proposition 1. *Let E/K be an elliptic curve.*

(1) *If* $\operatorname{char} K = 0$ *or if* $\operatorname{char} K = p, p$ *not dividing* n*, then*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

(2) *If* $\operatorname{char} K = p > 0$*, then*

$$E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z} \text{ or } 0$$

If E is defined over K then $E[n]$ is defined over its algebraic closure $\bar{K}$, and we can consider the associated Galois action. The action of Galois commutes with the group law on E so if $\operatorname{char} K = 0$ or if $\operatorname{char} K = p$, p not dividing n, then we get a homomorphism:

$$\rho : \operatorname{Gal}(\bar{K}/K) \to \operatorname{Aut}(E[n]) \simeq GL_2(\mathbb{Z}/n\mathbb{Z})$$

So this is a restriction. However, is this the only restriction? The answer is no, there is an additional restriction coming from the Weil Pairing.

1. Weil Pairing

The Weil pairing is a construction of roots of unity by means of functions on an elliptic curve E, in such a way as to constitute a pairing on the torsion subgroup of E, $E[n]$. We assume $\operatorname{char} K = 0$ or $\operatorname{char} K = p, p$ not dividing n throughout. Define

$$e_n : E[n] \times E[n] \to \mu_n$$

where, μ_n denotes the group of n-th roots of unity, and the map e_n is:

(1) Bilinear: $e_n(P+Q,R) = e_n(P,R)e_n(Q,R)$
(2) Galois Equivariant: For $\sigma \in \operatorname{Gal}(\bar{K}/K)$, $\sigma(e_n(P,Q)) = e_n(\sigma P, \sigma Q)$
(3) Non-degenerate: $e_n(P,Q) = 1,\ \forall P \in E[n] \implies Q = \mathcal{O}$

Galois equivariance implies that

$$det(\rho) : \operatorname{Gal}(\bar{K}/K) \to (\mathbb{Z}/n\mathbb{Z})^*$$

is the "cyclotomic character". So, $det(\rho(\sigma)) = a \in \mathbb{Z}/n\mathbb{Z}$ where a is such that $\sigma(\zeta) = \zeta^a\ \forall \zeta \in \mu_n$. This imposes an additional constraint on the Galois action on n-torsion points.

Theorem 1. *There exists a pairing with the above properties.*

Corollory 1. *If $E[n] \subset E[K]$, then $\mu_n \subset K$.*

Lets look at some examples to understand the restriction.
Example 1: When $n = 3$, over $\bar{K}$, $E[n] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. We have: $[K(E[n]) : K] \leq 9!$ but actually $\leq 8!$ since $\mathcal{O} \in E$. But $\#GL_2(\mathbb{Z}/3\mathbb{Z}) = (9-1)(9-3) = 48$, so $[K(E[n]) : K] \leq 48$.
Example 2: Let $K = \mathbb{R}$. $E[3] \cap E(\mathbb{R}) \simeq \mathbb{Z}/3\mathbb{Z}$. Note that we never get $E[3] \cap E(\mathbb{R}) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ because $\mathbb{R}$ does not contain a nontrivial cube root of unity (by Corollary).

Now, let C be an algebraic curve over an algebraically closed field K. Suppose $D = \sum n_P P$ is a divisor on C and $f \in K(C)^*$ such that f does not have zeros and poles on points that appear in D. I.e. $\operatorname{Supp}(D) \cap \operatorname{Supp}(f) = \emptyset$ where $\operatorname{Supp}(D) = \{P \in C | n_P \neq 0\}$. Define $f(D) = \prod f(P)^{n_P} \in K^*$.

Theorem 2. *Weil's Reciprocity Law: If $f, g \in K(C)^*$ with $\mathrm{Supp}(f) \cap \mathrm{Supp}(g) = \emptyset$, then $f((g)) = g((f))$.*

Weil Pairing: Let $P, Q \in E[n]$. Choose $D_P \sim [P - \mathcal{O}]$ and $D_Q \sim [Q - \mathcal{O}]$ with $\mathrm{Supp}(D_P) \cap \mathrm{Supp}(D_Q) = \emptyset$. E.g., let $D_P = (P + P_0) - (P_0)$ and $D_Q = Q - \mathcal{O}$. Then, $\exists f, g,\ s.t. (f) = nD_P, ;\ (g) = nD_Q$.

Define $e_n(P, Q) := \frac{f(D_Q)}{g(D_P)}$. The Weil reciprocity law is used to guarantee that $e_n(P, Q)$ is indeed an n^{th} root of unity, as follows:

$$\begin{aligned} e_n(P,Q)^n &= \Big(\frac{f(D_Q)}{g(D_P)}\Big)^n \\ &= \frac{f(D_Q)^n}{g(D_P)^n} \\ &= \frac{f(nD_Q)}{g(nD_P)} \\ &= \frac{f((g))}{g((f))} \\ &= 1 \end{aligned}$$

Note that the map e_n is well defined. To see this note that if we use the divisor $D_P + (h)$ instead of D_P, then f is changed to fh^n (since $(fh^n) = (f) + n(h) = n(D_P + (h))$).

So now,

$$\begin{aligned} e_n(P,Q) &= \frac{fh^n(D_Q)}{g(D_P + (h))} \\ &= \frac{f(D_Q)h(nD_Q)}{g(D_P)g((h))} \\ &= \frac{f(D_Q)}{g(D_P)} \cdot \frac{h((g))}{g((h))} \end{aligned}$$

We need to show Bilinearity, Galois Equivariance, non-degeneracy. We leave these as exercises.

We now prove the Weil Reciprocity Law:

Proof. We restrict attention to the case $K(f, g) = K(C)$. It can be shown that considering this case is sufficient (exercise).

So, suppose that $K(f, g) = K(C)$. Then, $\exists$ an irreducible equation $\sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} f^i g^j = 0$.

$$\begin{aligned} f((g)) &= \prod_P f(P)^{ord_P g} \\ &= \frac{\prod_{ord_P g > 0} f(P)^{ord_P g}}{\prod_{ord_P g < 0} f(P)^{-ord_P g}}. \end{aligned}$$

If $g(P) = 0$, then $\sum_{i=0}^{n} a_{i0} f(P)^i = 0$. The roots of the equation

$$\sum_{i=0}^{n} a_{i0} x^i = 0$$

are the values of f on the zeros of g.

$$\prod_{ord_P g>0} f(P)^{ord_P g} = (-1)^n \frac{a_{00}}{a_{n0}}.$$

If $g(P) = \infty$, then $(1/g)(P) = 0$, and

$$\sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij} f^i \left(\frac{1}{g}\right)^{m-j} = 0.$$

Hence $f(P)$ satisfies

$$\sum_{i=0}^{n} a_{im} f(P)^i = 0$$

$$\Rightarrow \prod_{ord_P g<0} f(P)^{-ord_P g} = (-1)^n \frac{a_{00}}{a_{0m}}.$$

Similarly,

$$\prod_{ord_P f>0} g(P)^{ord_P f} = (-1)^m \frac{a_{00}}{a_{0m}}$$

$$\prod_{f(P)=\infty} g(P)^{-ord_P f} = (-1)^m \frac{a_{n0}}{a_{nm}}$$

Thus,

$$\frac{f((g))}{g((f))} = \frac{(-1)^n \frac{a_{00}}{a_{n0}}}{(-1)^n \frac{a_{0m}}{a_{nm}}} \left(\frac{(-1)^m \frac{a_{00}}{a_{0m}}}{(-1)^m \frac{a_{n0}}{a_{nm}}}\right)^{-1}$$
$$= 1.$$

□

Remark: If K is not algebraically closed and $f \in K(C)$ and D is a divisor on C defined over K such that $\mathrm{Supp}(f)) \cap \mathrm{Supp}(D) = \emptyset$, then $f(D) \in K$, and Weil reciprocity works over K also.

Example: Let $f(x), g(x) \in \mathbb{F}_q[x]$ be irreducible, monic, distinct polynomials, with q an odd prime. Letting $h(x) = f(x)/x^{deg(f)}$, we have

$$(h) = \left(\frac{f(x)}{x^{deg f}}\right) = \sum_{f(\alpha)=0} (\alpha) - deg(f)(0)$$

$$(g) = \sum_{g(\beta)=0} (\beta) - deg(g)(\infty).$$

By Weil reciprocity,

$$\frac{h((g))}{g((h))} = 1 = \frac{\left(\prod_{g(\beta)=0} \frac{f(\beta)}{\beta^{deg(f)}}\right)(h(\infty))^{-deg(g)}}{\left(\prod_{f(\alpha)=0} g(\alpha)\right)(g(0))^{-deg(f)}}$$

$$= \frac{\prod_{g(\beta)=0} f(\beta)}{\prod_{f(\alpha)=0} g(\alpha)} (-1)^{deg(g)deg(f)}. \tag{1}$$

Note that $\mathbb{F}_q[x]/(f(x)) \cong \mathbb{F}_{q^{deg(f)}}$, from the homomorphism $x \mapsto \alpha$; assuming $deg(f) = n$, the roots of f are $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$. We have

$$\begin{aligned}\prod_{i=0}^{n-1} g(\alpha^{q^i}) &= g(\alpha)^{\sum_{i=0}^{n-1} q^i} \\ &= g(\alpha)^{\frac{q^n-1}{q-1}} \\ &= g(x)^{\frac{q^n-1}{q-1}} \mod f(x), \end{aligned} \tag{2}$$

and $g(x)^{\frac{q^n-1}{q-1}} \mod f(x) = 1$ if and only if $g(x)$ is a $(q-1)$-th power in $\mathbb{F}_q[x]/(f(x))$.

For a polynomial $p(x) \in F_q[x]/(f(x))$, we have $p^{(q^n-1)/2} = \pm 1 \bmod f(x)$. Define the *Legendre symbol*

$$\left(\frac{p}{f}\right)_2 \equiv p^{(q^n-1)/2} \bmod f \ \in \{-1, +1\}.$$

Thus, (1) and (2) imply

$$\left(\frac{f}{g}\right)_2 = \left(\frac{g}{f}\right)_2 (-1)^{(\frac{q-1}{2})deg(f)deg(g)},$$

which is called *quadratic reciprocity* in $\mathbb{F}_q[x]$.

2. Invariant Differential

Consider an elliptic curve E over K with associated Weierstrass equation

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

We have that the differential

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

is holomorphic and non-vanishing, i.e. $\operatorname{div}(\omega) = 0$. Let $\operatorname{char} K \neq 2, 3$, and considering the equivalent form

$$y^2 = x^3 + c_4x + c_6,$$

we have $\omega = \frac{dx}{2y}$ in this case. Changing x to $\lambda^2 x$ and y to $\lambda^3 y$, $\omega = \frac{dx}{2y}$ changes to $\lambda^{-1}\frac{dx}{2y}$.

Recall the translation map

$$\begin{aligned}\tau_{P_0} : E &\longrightarrow E \\ P &\longmapsto P + P_0.\end{aligned}$$

Theorem 3. *For every $P_0 \in E$, $\tau_{P_0}^* \, \omega = \omega$.*

Proof. Firstly, we note that $\tau_{P_0}^{-1} = \tau_{-P_0}$, so τ_{P_0} is an isomorphism of curves; thus $\tau_{P_0}^* \, \omega$ is also a holomorphic differential.

E has genus 1, so the space of differential forms without poles has dimension 1 over K. Hence, there exists $a_{P_0} \in K$ such that $\tau_{P_0}^* \, \omega = a_{P_0} \, \omega$.

Let us consider the map $P_0 \longmapsto a_{P_0}$ as a map $E \longrightarrow \mathbb{A}^1$. This is a rational map which is defined everywhere, so it is a regular map. But E is projective and $\mathbb{A}^1$ is affine, so this map must be constant. Using the fact that $\tau_{\mathcal{O}}$ is the identity, we have that $a_{\mathcal{O}} = 1$, implying that $a_{P_0} = 1 \ \forall \ P_0 \in E$. Thus, $\tau_{P_0}^* \ \omega = \omega$ and we are done. □

Let us now look at the elliptic curve from the complex-analytic point of view. Assuming $K = \mathbb{C}$, $E(\mathbb{C})$ becomes a compact Riemann surface. Let ω be an invariant differential on E. Define

$$\Lambda := \left\{ \int_\gamma \omega \ : \ \gamma \in \pi_1(E(\mathbb{C})) \right\} \subset \mathbb{C}.$$

Here γ represents all closed paths. Λ is a subgroup of $(\mathbb{C}, +)$. Let us look at $\mathbb{C}/\Lambda$.

Define

$$\begin{aligned} \phi : E(\mathbb{C}) &\longrightarrow \mathbb{C}/\Lambda \\ P &\longmapsto \int_{\mathcal{O}}^{P} \omega \mod \Lambda \end{aligned}$$

By the definition of Λ, this map is well-defined (ϕ is called the *Abel-Jacobi map*).

Theorem 4. *$\mathbb{C}/\Lambda$ is a compact Riemann surface, and ϕ is a biholomorphic group homomorphism.*

Proof. Let $t = x/y$ be a local parameter on E near $\mathcal{O}$. Then,

$$\begin{aligned} x &= t^{-2} + \cdots, \ \text{ and} \\ y &= t^{-3} + \cdots \end{aligned}$$

So we have

$$\begin{aligned} \frac{dx}{2y} &= \frac{(-2t^{-3} + \cdots)dt}{2(-t^{-3} + \cdots)} \\ &= -(1 + \cdots)dt \\ \Rightarrow \phi(t) &= \int_{\mathcal{O}}^{P_t} -(1 + \cdots)dt \\ &= -t + \cdots. \end{aligned}$$

Also, ϕ is a homomorphism because

$$\begin{aligned} \phi(P + Q) &= \int_{\mathcal{O}}^{P+Q} \omega \\ &= \int_{\mathcal{O}}^{P} \omega + \int_{P}^{P+Q} \omega \\ &= \int_{\mathcal{O}}^{P} \omega + \int_{\mathcal{O}}^{Q} \tau_{-P}^* \ \omega \\ &= \int_{\mathcal{O}}^{P} \omega + \int_{\mathcal{O}}^{Q} \omega \\ &= \phi(P) + \phi(Q) \mod \Lambda. \end{aligned}$$

□

A local isomorphism which is a group homomorphism is an isomorphism. We will now compute ϕ^{-1}:

$$\phi^{-1} : \mathbb{C}/\Lambda \longmapsto E(\mathbb{C}),$$

$$\wp(z) \equiv \frac{1}{z^2} + \sum_{\substack{\lambda\in\Lambda,\\ \lambda\neq 0}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Λ is a discrete rank-2 subgroup of $\mathcal{C}$. $\wp(z)$ is holomorphic in $\mathbb{C}/\Lambda$, has double poles in the points of Λ and is Λ-periodic, i.e. $\wp(z+\lambda) = \wp(z)$. Consider now

$$\psi : z \longmapsto \left(\wp(z), \frac{1}{2}\wp'(z) \right).$$

Using complex-analytic arguments, it can be shown that $\psi : \mathbb{C}/\Lambda \longrightarrow \mathbb{A}^2$ extends to $\mathbb{C} \longrightarrow \mathbb{P}^2$, periodic to $\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2$. The image is an elliptic curve isomorphic to E, so ψ is essentially ϕ^{-1}.

It is possible by changing coordinates in $\mathbb{C}$ to change Λ to a lattice of the form $\mathbb{Z} + \mathbb{Z}\tau$, $\mathrm{Im}(\tau) > 0$. $\{1, \tau\}$ is a basis for Λ, and so is $\{a\tau + b, c\tau + d\}$ if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. So, $\{1, \frac{a\tau+b}{c\tau+d}\}$ also gives the same E.

ELLIPTIC CURVES OVER $\mathbb{C}$ (CONTINUED)

FELIPE VOLOCH
FEB 18, 2010
(NOTES BY YUAN YAO)

1. Isogenies

Proposition 1.1. *Let E_1, E_2 be two elliptic curves over $\mathbb{C}$, Λ_1, Λ_2 the corresponding lattices. Then $f : E_1 \to E_2$ is an isogeny if and only if there is a complex number α with $\alpha\Lambda_1 \subseteq \Lambda_2$, so that f is compatible with the induced map $\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ induced by multiplication by α on $\mathbb{C}$.*

Proof. The sufficiency is obvious. For the necessity, pick holomorphic differential ω_1, ω_2 on E_1, E_2 respectively. Denote the corresponding Abel-Jacobi maps by φ_1, φ_2. Then we have the commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{f} & E_2 \\ {\scriptstyle\varphi_1}\downarrow & & {\scriptstyle\varphi_2}\downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{g} & \mathbb{C}/\Lambda_2 \end{array}$$

Here g satisfies $g(\varphi_1(P)) = \varphi_2(f(P))$ for any $P \in E_1$. So $g(\int_{\mathcal{O}}^{P} \omega_1) = \int_{\mathcal{O}}^{f(P)} \omega_2 = \int_{\mathcal{O}}^{P} f^*\omega_2$. Notice that $f^*\omega_2$ is a holomorphic differential form on E_1, so there must exist $\alpha \in \mathbb{C}$ such that $f^*\omega_2 = \alpha\omega_1$. Then $g(\int_{\mathcal{O}}^{P} \omega_1) = \int_{\mathcal{O}}^{P} \alpha\omega_1 = \alpha \int_{\mathcal{O}}^{P} \omega_1$, g is just multiplication by α. □

In particular, if we set $E_1 = E_2 = E$, then "the ring of endomorphisms of E", denoted by $\mathrm{End}(E)$, would be same as $\{\alpha \in \mathbb{C} | \alpha\Lambda \subseteq \Lambda\}$. $\mathbb{Z}$ is always a subset of $\mathrm{End}(E)$, and we call elements in $\mathrm{End}(E)\backslash\mathbb{Z}$ (if it is nonempty) "complex multiplications" of E.

Example 1.2. Take $\Lambda = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. Then any $\alpha \in \mathbb{Z}[i]$ satisfies $\alpha\Lambda \subseteq \Lambda$. So $\mathbb{Z}[i]$ can be embedded into $\mathrm{End}(\mathbb{C}/\mathbb{Z}[i])$. Actually this is a bijective.

Example 1.3. The isogeny $[n] : E \to E$ corresponds to the case $\alpha = n$, which is not a complex multiplication. Using the lattice language, $E[n]$ is simply $\frac{1}{n}\Lambda/\Lambda \simeq (\mathbb{Z}/n\mathbb{Z})^2$. If $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, then $E[n] = \{\frac{a+b\tau}{n} | 0 \leq a, b \leq n-1\}$, and Weil pairing can be expressed as $e_n(\frac{a+b\tau}{n}, \frac{c+d\tau}{n}) = \exp(2\pi i \frac{ad-bc}{m})$.

Now suppose $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ is a lattice, $\alpha \in \mathbb{C}$ induces a complex multiplication of $E = \mathbb{C}/\Lambda$, i.e., $\alpha\Lambda \subseteq \Lambda$ and $\alpha \notin \mathbb{Z}$. Then $\alpha \cdot 1, \alpha \cdot \tau \in \Lambda$, so there are integers a, b, c, d such that $\alpha = a + b\tau, \alpha\tau = c + d\tau$. Then

we get $(a+b\tau)\tau = c+d\tau$, which is equivalent to the quadratic equation $b\tau^2+(a-d)\tau-c=0$. So $\mathbb{Q}(\tau)$ is extension of $\mathbb{Q}$ with degree at most 2. It can be shown that E itself can be defined over $\bar{\mathbb{Q}}$. In general, every elliptic curve over an arbitrary field with complex multiplication can be defined over the algebraic closure of the prime subfield. (I might prove this later.)

2. Tate curve

Given $\tau \in \mathbb{H}$, let $q = \exp(2\pi i\tau)$, then $0 < |q| < 1$ since $\mathrm{Im}(\tau) > 0$. Set E_q as the elliptic curve corresponding to the lattice $\mathbb{Z}+\mathbb{Z}\tau$, then the j-invariant of E_q can be written as $j = q^{-1} + 744 + \sum_{n\geq 1} c_n q^n$. The equation of E_q would be $y^2+xy = x^3+a_4x+a_6$, where

$$a_4 = -5\sum_{n\geq 1}\frac{n^3q^n}{1-q^n},\ a_6 = -\frac{1}{12}\sum_{n\geq 1}\frac{(7n^5+5n^3)q^n}{1-q^n}.$$

Theorem 2.1. *The above equation (varying $0<|q|<1$) gives us all elliptic curves over $\mathbb{C}$. And for each $0<|q|<1$, $\mathbb{C}^\times/q^{\mathbb{Z}}$ has a biholomorphic isomorphism (as groups) to $E_q(\mathbb{C})$ via*

$$u \mapsto \begin{cases} (x(u,q), y(u,q)) & , \quad u \neq 1 \\ \mathcal{O} & , \quad u = 1 \end{cases}$$

where

$$x(u,q) = \sum_{n\in\mathbb{Z}}\frac{q^nu}{(1-q^nu)^2} - 2\sum_{n\in\mathbb{Z}}\frac{nq^n}{1-q^n},$$

$$y(u,q) = \sum_{n\in\mathbb{Z}}\frac{q^{2n}u^2}{(1-q^nu)^3} + \sum_{n\in\mathbb{Z}}\frac{nq^n}{1-q^n}.$$

Proof. Every elliptic curve over $\mathbb{C}$ can be associated with some lattice $\mathbb{Z}+\mathbb{Z}\tau$ with $\tau\in\mathbb{H}$, so the above process generates all elliptic curves over $\mathbb{C}$. This implies the first statement. For the second, notice that $\psi : \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau) \to \mathbb{C}^\times/q^{\mathbb{Z}} : z \mapsto \exp(2\pi i z)$ is a biholomorphic isomorphism of groups, and so is the inverse of Abel-Jacobi map $\varphi^{-1} : \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau) \to E_q(\mathbb{C}) : z \mapsto (\wp(z), \frac{1}{2}\wp'(z))$. Then the composition $\varphi^{-1}\circ\psi^{-1} : \mathbb{C}^\times/q^{\mathbb{Z}} \to E_q(\mathbb{C})$ is also a biholomorphic isomorphism of groups, and gives us the expression of $(x(u,q), y(u,q))$ in the theorem. □

Remark 2.2. The formulas in the theorem make sense (and converge) in any complete valued field K with $q\in K$, $0<|q|<1$. But if K is a non-archimedean valued field (say $K=\mathbb{Q}_p$ or $K=k((t))$), we are not able to get all elliptic curves over K using those equations. Instead, we only get elliptic curves E over K whose j-invariant satisfies $|j(E)|>1$. The elliptic curves thus obtained are called Tate curves with parameter q. As a special case, let k be a field, $K=k((q))$ be the field of formal Laurent series on the variable q over k, endowed with the standard non-archimedean norm. Then $K^\times/q^{\mathbb{Z}}$ is a Tate curve over K.

This can be viewed as a generalization of usual elliptic curves over $\mathbb{C}$. Inspired by the above theorem, we also have the following

Let q_1, q_2 be two parameters in K, non-archimedean complete field, $E_{q_1} := K^\times/q_1^{\mathbb{Z}}$ and $E_{q_2} := K^\times/q_2^{\mathbb{Z}}$ be the corresponding Tate curves. A map $f : E_{q_1} \to E_{q_2}$ is called an isogeny if it is a group homomorphism. Fix $E_q = K^\times/q^{\mathbb{Z}}$ and $n \in \mathbb{Z}$, then we have the natural isogeny to itself: $[n] : K^\times/q^{\mathbb{Z}} \to K^\times/q^{\mathbb{Z}} : u \mapsto u^n$. It factors as a composition of the isogenies $K^\times/q^{\mathbb{Z}} \to K^\times/q^{n\mathbb{Z}} : u \mapsto u^n$ and $K^\times/q^{n\mathbb{Z}} \to K^\times/q^{\mathbb{Z}} : u \mapsto u$.

Again set $E[n] = \ker([n])$, then $E[n] = \{\zeta^a(q^{1/n})^b | 0 \le a, b \le n-1\}$, where ζ is a primitive n-th root of 1, and $q^{1/n}$ is a n-th root of q in $\overline{K} = \overline{k((q))}$. This gives us the following exact sequence of group schemes (μ_n is the set of n-th roots of 1):

$$0 \longrightarrow \mu_n \longrightarrow E[n] \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

Proposition 2.3. *Let E_1, E_2 be two Tate curves over K, q_1, q_2 the corresponding parameters. Then $f : E_1 \to E_2$ is an isogeny if and only if there are integers n_1, n_2 with $q_1^{n_1} = q_2^{n_2}$, so that f is given by $K^\times/q_1^{\mathbb{Z}} \to K^\times/q_2^{\mathbb{Z}} : u \mapsto u^{n_1}$.*

Proof. Sufficiency: we only need to verify that the map is well-defined. Suppose $u_1, u_2 \in K^\times$ satisfies $u_1 = q_1^n u_2$, n is an integer. Then $u_1^{n_1} = (q_1^n u_2)^{n_1} = q_1^{n_1 n} u_2^{n_1} = (q_1^{n_1})^n u_2^{n_1} = (q_2^{n_2})^n u_2^{n_1} = q_2^{n_2 n} u_2^{n_1}$. So f is well-defined.

Necessity: not presented. □

Corollory 2.4. *For the Tate curve $E = K^\times/q^{\mathbb{Z}}$, over the Laurent series field $k((q))$, the ring of endomorphisms* $\mathrm{End}(E) \simeq \mathbb{Z}$.

Proof. $q^{n_1} = q^{n_2}$ in $k((q))$ implies $n_1 = n_2$. □

MODULAR CURVES

FELIPE VOLOCH
FEB 23, 2010
(NOTES BY YUAN YAO)

1. Level structure

We want to study the moduli space of elliptic curves together with some specific structure related to their torsion. These structures are called "level structure", and have the following standard examples:

Definition 1.1. Fix a field K and an integer $N \geq 2$ with $\mathrm{char}(K) \nmid N$. Fix a primitive N-th root ζ of 1. A $\Gamma(N)$-structure on an elliptic curve E is a pair (P_1, P_2) of points, satisfying $P_1, P_2 \in E[N]$ and $e_N(P_1, P_2) = \zeta$. A $\Gamma_1(N)$-structure on E is a point P of order exactly N. A $\Gamma_0(N)$-structure on E is a cyclic subgroup C of order N.

In order to develop a moduli theory, we also need to define "isomorphisms":

Definition 1.2. Let E, E' be two elliptic curves, (P_1, P_2) a $\Gamma(N)$-structure on E and (P_1', P_2') a $\Gamma(N)$-structure on E' (resp. P a $\Gamma_1(N)$-structure on E and P' a $\Gamma_1(N)$-structure on E', resp. C a $\Gamma_0(N)$-structure on E and C' a $\Gamma_0(N)$-structure on E'). We say there is an isomorphism $(E, P_1, P_2) \simeq (E', P_1', P_2')$ (resp. $(E, P) \simeq (E', P')$, resp. $(E, C) \simeq (E', C')$) if there is an isomorphism $f : E \to E'$ of elliptic curves so that $(f(P_1), f(P_2)) = (P_1', P_2')$ (resp. $f(P) = P'$, resp. $f(C) = C'$).

Example 1.3. Given an elliptic curve E, the map $f : E \to E : P \mapsto -P$ is an isomorphism of E, and $e_N(-P_1, -P_2) = e_N(P_1, P_2)^{(-1)^2} = e_N(P_1, P_2)$, so f gives isomorphisms $(E, P) \simeq (E, -P)$, $(E, P_1, P_2) \simeq (E, -P_1, -P_2)$. In general, if φ is an automorphism of E, then $(E, P) \simeq (E, \varphi(P))$, and $(E, P_1, P_2) \simeq (E, \varphi(P_1), \varphi(P_2))$ holds if and only if $e_N(\varphi(P_1), \varphi(P_2)) = e_N(P_1, P_2)$.

We have the following result on the automorphism group of a given elliptic curve:

Proposition 1.4. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over field K with $\mathrm{char}(K) \neq 2, 3$. If $a \neq 0$ and $b \neq 0$, then $\mathrm{Aut}(E) = \{\pm 1\}$; if $a = 0$ and $b \neq 0$, then $\mathrm{Aut}(E)$ is a cyclic group of order 6; if $a \neq 0$ and $b = 0$, then $\mathrm{Aut}(E)$ is a cyclic group of order 4. (Since E is an elliptic curve, a, b can not be 0 simultaneously.)*

Proof. $\mathrm{Aut}(E) = \{\varphi : E \to E \mid \varphi \text{ is an isomorphism}\} = \{\varphi : E \to E : (x,y) \mapsto (\lambda^2 x, \lambda^3 y) \mid \lambda^4 a = a, \lambda^6 b = b\} \simeq \{\lambda \mid \lambda^4 a = a, \lambda^6 b = b\} = \begin{cases} \{\lambda \mid \lambda^4 = \lambda^6 = 1\} = \{\lambda \mid \lambda^2 = 1\} = \{\pm 1\} & , \quad a \neq 0, b \neq 0 \\ \{\lambda \mid \lambda^6 = 1\} = \mu_6 & , \quad a = 0, b \neq 0 \\ \{\lambda \mid \lambda^4 = 1\} = \mu_4 & , \quad a \neq 0, b = 0 \end{cases}$ □

2. Modular curves

Now we are ready to work on the moduli spaces of triples (E, P_1, P_2), pairs (E, P) or pairs (E, C) up to isomorphisms defined above. They are called "modular curves". The word "curve" comes from the following

Main Theorem 2.1. *Fix a field K and an integer $N \geq 2$ with $\mathrm{char}(K) \nmid N$. Fix a primitive N-th root ζ of 1. Then there exist smooth irreducible affine curves $Y(N)$, $Y_1(N)$, $Y_0(N)$ which are coarse moduli spaces for the corresponding level structure $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$. $Y(N)$ is defined over $K(\zeta)$, and $Y_1(N)$, $Y_0(N)$ are defined over K (see the remark below). Moreover, when $N \geq 3$, $Y(N)$ is also a fine moduli space; and when $N \geq 5$, $Y_1(N)$, is also a fine moduli space.*

$Y_0(N)$ is never a fine moduli space.

Fact 2.2. The congruence subgroups of the "modular group" $SL_2(\mathbb{Z})$ are:

$$\Gamma(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \bmod N,\ b \equiv c \equiv 0 \bmod N\},$$

$$\Gamma_1(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \bmod N,\ c \equiv 0 \bmod N\},$$

$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod N\}.$$

Then the $\mathbb{C}$-points of $Y(N)$, $Y_1(N)$, $Y_0(N)$ have the same topological structure with the quotient of $\mathbb{H}$ by the action of corresponding congruence subgroups:

$$\mathbb{H}/\Gamma(N) \simeq Y(N)(\mathbb{C}) : \tau \mapsto (\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \frac{1}{N}, \frac{\tau}{N}),$$

$$\mathbb{H}/\Gamma_1(N) \simeq Y_1(N)(\mathbb{C}) : \tau \mapsto (\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \frac{1}{N}),$$

$$\mathbb{H}/\Gamma_0(N) \simeq Y_0(N)(\mathbb{C}) : \tau \mapsto (\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \langle\frac{1}{N}\rangle).$$

Remark 2.3. In the main theorem, for $\Gamma(N)$ or $\Gamma_1(N)$, "defined over" a field means in the triple (E, P_1, P_2) or pair (E, P) presented by a point in the moduli space, both the elliptic curve E and points P_1, P_2, P are defined over that field; while for $\Gamma_0(N)$, "defined over K" means in the pair (E, C) presented by a point in the moduli space, the elliptic curve E is defined over K, and the group C is $\mathrm{Gal}(\overline{K}/K)$-invariant.

Remark 2.4. We can further consider the projective closure of $Y(N)$, $Y_1(N)$, $Y_0(N)$, denoted by $X(N)$, $X_1(N)$, $X_0(N)$ respectively. This process can be also viewed as a compactification of the corresponding quotient space given in the Fact above. The added points are called cusps.

Example 2.5. For $N = 2$, $\mathrm{char}(K) \neq 2$ and $\zeta = -1$, we can show directly that $Y(2) \simeq \mathbb{A}^1 - \{0, 1\}$: a point in $Y(2)$ is given by (E, P_1, P_2) with E an elliptic curve and P_1, P_2 points on E. E can be expressed as a cubic with P_1, P_2 its roots. By changing coordinates, we can assume $P_1 = (0, 0)$, $P_2 = (1, 0)$ and E would become $y^2 = x(x-1)(x-\lambda)$. Then the map $(E, P_1, P_2) \mapsto \lambda$ sets an isomorphism from $Y(2)$ to $\mathbb{A}^1 - \{0, 1\}$.

3. Proof of main theorem

We will struggle for a proof of the main theorem in the following several classes. Although long and complicated, the whole proof is subject to one philosophy:

How would we write down equations for $Y(N)$?

As a toy model, write E as $y^2 = x^3 + ax + b$, and the isogeny $[n]$ can be expressed as rational functions, or more explicitly, $[n](x, y) = (\frac{A_N(x)}{F_N^2(x)}, \frac{yB_N(x)}{F_N^3(x)})$ for some polynomials $A_N(x), B_N(x), F_N(x)$. Then condition $F_N(x_0) = 0$ means the point (x_0, y_0) has an order dividing N. There should be a factor of $F_N(x)$, say $G_N(x)$, describing the condition that the point has order exactly N. Then basically, the equations we want are $y^2 = x^3 + ax + b$, $G_N(x_1) = G_N(x_2) = 0$, and another equation describing $e_N(P_1, P_2) = \zeta$.

We will use the following theorem to prove our main theorem:

Theorem 3.1. *Fix a field K and an integer $N \geq 2$ with $\mathrm{char}(K) \nmid N$. Suppose there is a primitive N-th root ζ of 1 with $\zeta \in K$. Let E be an elliptic curve over $K(t)$ with j-invariant t. Let $F_N \subseteq \overline{K(t)}$ be the field generated by the coordinates of all N-torsion points of E in $\overline{K(t)}$ over $K(t)$. Then F_N is finite Galois over $K(t)$, K is algebraically closed in F_N, and $\mathrm{Gal}(F_N/K(t)) \simeq SL_2(\mathbb{Z}/N\mathbb{Z})$.*

Corollary 3.2. *If $\zeta \notin K$, then $\mu_N \cap K = \mu_d$ for some $d|N$. Moreover, d is the largest number so that $\mathrm{Gal}(F_N/K(t)) = \{\gamma \in GL_2(\mathbb{Z}/N\mathbb{Z}) \mid \det\gamma$ acts trivially on $\mu_d\}$.*

Let us first make some observations. We know $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ as groups, and any $\sigma \in \mathrm{Gal}(F_N/K(t))$ has a natural action on $E[N]$ satisfying $\sigma(P+Q) = \sigma(P)+\sigma(Q)$, since the group law is defined over $K(t)$. Choose a basis $\{P_1, P_2\}$ of $E[N]$, then $\zeta := e_N(P_1, P_2)$ is a N-th root of 1. Moreover, under the basis $\{P_1, P_2\}$, σ determines a matrix $\rho(\sigma) \in GL_2(\mathbb{Z}/N\mathbb{Z})$, and the map $\sigma \mapsto \rho(\sigma)$ sets an embedding of $\mathrm{Gal}(F_N/K(t))$ into $GL_2(\mathbb{Z}/N\mathbb{Z})$. Suppose $\sigma(P_1) = aP_1 + bP_2$, $\sigma(P_2) = cP_1 + dP_2$, then $\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

and $\sigma(e_N(P_1,P_2)) = e_N(\sigma(P_1),\sigma(P_2)) = e_N(P_1,P_2)^{(ad-bc)}$. So if $\zeta \in K$, we would have $\det \rho(\sigma) = ad - bc = 1$.

In order to prove the corollary, we do the same calculations with P_1, P_2 replaced by $\frac{N}{d}P_1, \frac{N}{d}P_2$.

(to be continued)

1 Notes 02/25/10

Corrections: Corrections from previous notes.

1. $Y(2) = \mathbb{A}^1 \setminus \{0,1\} = \mathbb{P}^1 \setminus \{0,1,\infty\}$
2. $Y_0(N)$ is never a fine moduli space.

We state a few result whose proof will be given later.

Theorem. *Let E be an elliptic curve over $K(t)$ (t a variable) with j-invariant t. Let F_N be the field obtained by adjoining the coordinates of the points in $E[N]$ to $K(t)$. Then if $\zeta \in K$, $\mathrm{Gal}(F_N/K(t)) = SL_2(\mathbb{Z}/N)$ and K is algebraically closed in F_N.*

Corollary. *If $\zeta \notin K, \mu_N \bigcap K = \mu_d$. $\mathrm{Gal}(F_N/K(t))$ is the set of $\gamma \in GL_2(\mathbb{Z}/N)$ such that $\det\gamma$ acts trivially on μ_d*

Note that $GL_2(\mathbb{Z}/N)/SL_2(\mathbb{Z}/N))$ is isomorphic, via the determinant, to $(\mathbb{Z}/N)^\times$.

An automorphism φ of an elliptic curve E is an automorphism of E with $\Gamma(N)$ level structure (P_1, P_2) if $e_N(\varphi(P_1), \varphi(P_2)) = e_N(P_1, P_2)$. The last equality is true when $\varphi = \pm 1$, by the bilinearity of the Weil pairing. It turns out it is true for arbitrary φ, which can be checked directly by using the explicit description of elliptic curves with extra automorphisms.

Corollary. *Let K be a field with $charK = 0$ or $charK = p$ with $p \nmid N$. Let $\zeta \in K$. Let F_N^+ be the subfield of F_N fixed by $\{\pm I\} \subseteq SL_2(\mathbb{Z}/N)$. Then F_N^+ is the field obtained by adjoining the x-coordinates of points in $E[N]$ to $K(t)$. Let $X(N)/K$ be a smooth projective curve with function field F_N^+. Then there is an open affine subset of $X(N)$ which is a coarse moduli space for elliptic curves with $\Gamma(N)$ structure.*

We have a map $X(N) \to \mathbb{P}^1$ coming from $F_N^+ \supseteq K(t)$ where $t = j(E)$. Let $Y(N) = j^{-1}(\mathbb{A}^1)$. We want to prove that

1) $Y(N)(\bar{K})$ is in bijection with the set of isomorphism classes of elliptic curves over $\bar{K}$ with $\Gamma(N)$ structure;

2) Given a flat family $f : Y \to T$ of elliptic curves with $\Gamma(N)$ structure, there is a map $h : T \to Y(N)$ such that $f^{-1}(t)$ corresponds to $h(t)$ under the bijection in 1) for all $t \in T(\bar{K})$.

Recall that, by definition, a flat family of elliptic curves with level N structure consists of a flat map $f : Y \to T$ of varieties such that $f^{-1}(t)$ is a curve of genus one for all $t \in T$ having sections $o : T \to Y, p_1 : T \to Y, p_2 : T \to Y$ such that $E_t = (f^{-1}(t), o(t))$ is an elliptic curve and $(p_1(t), p_2(t))$ is a $\Gamma(N)$ structure on E_t.

Let $E : y^2 = x^3 + \frac{3t}{1728-t}x + \frac{2t}{1728-t}$. Here $j(E) = t$. For any $\alpha \in \bar{K}, \alpha \neq 0, 1728, E_\alpha$ is an elliptic curve with j-invariant α.

$E(F_N)$ contains $E[N]$. In particular, it contains $P_1, P_2 \in E[N]$ i with $e_N(P_1, P_2) = \zeta$. Note that P_1, P_2 are algebraic functions of t and for any

$\alpha \in \bar{K} \smallsetminus \{0, 1728\}$ we can specialize $t = \alpha$ and get $P_1(\alpha), P_2(\alpha)$ a $\Gamma(N)$ structure on E_α (i.e, choosing a point $Q_\alpha \in Y(N)(K(\alpha))$ above α). Note that this gives 1) above except for $j = 0, 1728$. So we get a map $\bar{K} \smallsetminus \{0, 1728\}$ to the isomorphism classes of elliptic curves over $\bar{K}$ with $\Gamma(N)$ structures with $j \neq 0, 1728$.

Conversely, suppose E' is an elliptic curve over $\bar{K}$ with $\Gamma(N)$ structure (P_1', P_2') and $j(E') \neq 0, 1728$. First of all, E' is isomorphic to E_α over $\bar{K}$ and $P_1(\alpha), P_2(\alpha)$ is a $\Gamma(N)$ structure on E_α. Now, there exists $a, b, c, d \in \mathbb{Z}/N$ such that $P_1' = aP_1(\alpha) + bP_2(\alpha)$ and $P_2' = cP_1(\alpha) + dP_2(\alpha)$. Also, $\zeta = e_N(P_1', P_2') = e_N(P_1(\alpha), P_2(\alpha))^{ad-bc} = \zeta^{ad-bc}$ which gives $ad - bc = 1$. By the theorem, $\mathrm{Gal}(F_N/K(t)) = SL_2(\mathbb{Z}/N)$ so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on $Y(N)$. So $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(Q_\alpha)$ makes sense where Q_α is the point corresponding to $E_\alpha, P_1(\alpha), P_2(\alpha)$ and is a point on $Y(N)$ corresponding to E'.

Given a flat family $f : Y \to T$ of elliptic curves with $\Gamma(N)$ structure we want to construct a map $T \to Y(N)$. Since $f^{-1}(t)$ is an elliptic curve for all t we have the j-invariant giving a map $j : T \to \mathbb{A}^1$. There is a $\Gamma(N)$ level structure over the elliptic curve $E'/K(U)$ where U is an open set of T. Note $t \in K(U)$. So: we can pull back E to U and E comes with a level structure over F_N. We now get a level structure over possibly an extension of $K(U)$.

2 Notes 03/02/10

Exercise: show that there exists $G_N \in \mathbb{Z}[c_4, c_6, x]$ such that (x_0, y_0) is a point of order exactly N in $y^2 + x^3 + c_4x + c_6$ if and only if $G_N(x_0) = 0$.

Consider the following system of equations in t, x_1, x_2:

$$c_4 = \frac{3t}{1728 - t} \tag{1}$$

$$c_6 = \frac{2t}{1728 - t} \tag{2}$$

$$P_i = (x_i, y_i) \tag{3}$$

$$G_N(x_1) = 0 \tag{4}$$

$$G_N(x_2) = 0 \tag{5}$$

$$e_N(P_1, P_2) = \zeta \tag{6}$$

This system of equations defines an irreducible curve.

Proof. This follows from $\mathrm{Gal}(F_N, K(t)) = SL_2(\mathbb{Z}/N)$ because if you take one point in $E[N]$ with coordinates in F_N then you get all others by Galois action. The degree of $X(N) \to \mathbb{P}^1$ is $\#SL_2(\mathbb{Z}/N)/\pm I$. $X(N)$ maps to a component of this system of equations by choosing a $\Gamma(N)$ structure since the map on this system to $\mathbb{P}^1$ given by t has degree at most $\#SL_2(\mathbb{Z}/N)/\pm I$. Then $X(N)$ has to be the whole of the system. □

Suppose we have a family $f : Y \to T$ of elliptic curves with $\Gamma(N)$ structure. So $y^2 = x^3 + c_4'x + c_6'$ with $c_4', c_6' \in K(T)$ and points $P_i = (x_i', y_i') \in E'(N)$ and

$x_i, y_i \in K(T)$. So now we have $e_N(P_1', P_2') = \zeta$. So we have a map $j : T \to \mathbb{P}^1$ by $\alpha \to\!\!\!\!\to j(f^{-1}(\alpha))$. We can then consider the curve $y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$, call it $j^\star E$. Now, by construction, $j(E') = j(j^\star E) = j$ except when $j = 0, 1728$. So: E' is a quadratic twist of $j^\star E$ so, without loss of generality, E' can be given by $dy^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$ for some d. Now we can use the $\Gamma(N)$ structure on E' to get a map $T \to X(N)$.

Earlier, we showed that there was a 1-1 coorespondence of isomorphism classes of elliptic curves with a $\Gamma(N)$ structure (with $j \neq 0, 1728$) and points in an open subset of $X(N)$.

Let $D = \#SL_2(\mathbb{Z}/N)/\pm I$. Then $D = \#j^{-1}(\alpha)$ except for $\alpha = 0, 1728, \infty$ and $\#j^{-1}(0) = D/3$ and $\#j^{-1}(1728) = D/2$, for $N \neq 2$.

To analyze $j = 0$ note that $j = 0$ corresponds to $t = 0$. Then, changing variables by $x = t^{1/3}x', y = t^{1/2}y'$ to get: $(y')^2 = (x')^3 + \frac{3t^{1/3}}{1728-t}x' + \frac{2}{1728-t}$. Now it is okay to have $t = 0$. So: we do the calculation in $K(t^{1/6})$.

Using the diagram for fields it is possible to show that the set of isomorphism classes of elliptic curves with $j = 0$ and $\Gamma(N)$ structure is in bijection with $j^{-1}(0) \subseteq X(N)$ in such a way that makes $Y(N)$ into a coarse moduli space.

A similar process is used for $j = 1728$.

To compute $D(N) = \#SL_2(\mathbb{Z}/N)/\pm I$, first we show that if $N = \prod p_i^{\alpha_i}$ then $\tilde{D}(N) = \prod \tilde{D}(p_i^{\alpha_i})$ where $\tilde{D}(N) = \#SL_2(\mathbb{Z}/N)$. Further, $\tilde{D}(p) = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1)$. i So: $D(p) = 6$ when $p = 2$ and $\tilde{D}(p)/2$ otherwise.

An example: $X(3) = \mathbb{P}^1_t$. We use the cubic curve $C_t : x^3 + y^3 + z^3 = txyz \subseteq \mathbb{P}^2$. Now, the points $(0 : 1 : -\omega), (1 : 0 : \omega), (1 : -\omega : 0)$ with $\omega^3 = 1$ are on C_t and, if we choose the point $(0 : 1 : -1)$ as the identity, then the other points listed have order 3.

Elliptic Curves

Notes taken by James Jones for Dr. Voloch

March 4, 2010

Let k be a field containing a primitive Nth root of unity ζ so that $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p \nmid N$. Let $E/k(t)$ be an elliptic curve with j-invariant t. Recall $F_N = k(t)(E[N])$ and $F_N^+ = k(t)(x(E[N]))$. Let $X(N)$ be the curve over k with function field F_N^+. Recall the claim that $\mathrm{Gal}(F_N/k(t)) \cong SL_2(\mathbb{Z}/N)$ (hence $SL_2(\mathbb{Z}/N)/\{\pm I\}$ acts on $X(N)$). Recall that it was proved that $Y(N) = X(N) \setminus j^{-1}(\infty)$ is a coarse moduli space for elliptic curves with $\Gamma[N]$-structure.

Define

$$H_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}/N) \right\}$$

and

$$H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_2(\mathbb{Z}/N) \right\}$$

and let H_1^+ and H_2^+ be their images in $SL_2(\mathbb{Z}/N)/\{\pm I\}$. Also define $X_1(N) = X(N)/H_1^+$ and $X_0(N) = X(N)/H_2^+$. Let $Y_1(N) = X_1(N) \setminus j^{-1}(\infty)$ and $Y_0(N) = X_0(N) \setminus j^{-1}(\infty)$.

Theorem 1. *$Y_1(N)$ and $Y_0(N)$ are coarse moduli spaces for elliptic curves with $\Gamma_1(N)$- and $\Gamma_0(N)$-structures respectively.*

Proof for $Y_1(N)$: Take a point $x \in Y_1(N)(\overline{k})$. Then there is a point in $Y(N)(\overline{k})$ mapping to x, so we have an $(E, P_1, P_2) \in Y(N)(\overline{k})$. Map $(E, P_1, P_2) \longmapsto (E, P_1)$. Then we must show that (E, P_1) is independent of the choice of P_2. The action of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/N)/\{\pm I\}$ on (E, P_1, P_2) is $(E, aP_1 + bP_2, cP_1 + dP_2)$. So the fiber over x in $Y(N)(\overline{k})$ is an orbit of

the action. The whole fiber over x is the orbit of (E, P_1, P_2) under H_1. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_1$, then $a = d = 1$ and $b = 0$ so $(E, P_1, cP_1 + P_2)$ is the image of (E, P_1, P_2) under the action. Hence, the choice of (E, P_1) is well-defined. Conversely, consider (E, P_1), where P_1 is a point of order N. There is $Q \in E[N]$ so that $\langle P_1, Q\rangle = E[N]$. This implies $e_N(P_1, Q) = \zeta^k$, which implies $(k, N) = 1$, so $e_N(P_1, k^{-1}Q) = \zeta$ and (E, P_1, Q) is a $\Gamma[N]$-structure. It remains to show the second condition for coarse moduli spaces, but it is done using essentially the same method of lifting to $Y[N]$. The proof for $Y_0(N)$ is similar as well.

In addition to this theorem, it is a fact that $Y(N)$ is a fine moduli space for $N \geq 3$, and $Y_1(N)$ is a fine moduli space for $N \geq 5$.

To show this, recall that $E/k(t)$ is an elliptic curve with j-invariant t. Then E/F_N^+ comes equipped with a $\Gamma[N]$-structure, and so can be regarded as a family of elliptic curves $\mathcal{E} = F \times_{\mathbb{P}^1} Y(N) \to Y(N)$, where $F : y^2 = x^3 + c_4x + c_6$, and $c_4 = \frac{3t}{1728-t}$ and $c_6 = \frac{2t}{1728-t}$. Now we want to show that family is unique up to isomorphisms of elliptic curves with $\Gamma[N]$-structure. So suppose $\mathcal{E}'$ is another such family. Then $\mathcal{E}$ and $\mathcal{E}'$ both have the same j-invariant, as elliptic curves over $k(T)$, hence they are twists of each other. There exists $\varphi : \mathcal{E} \to \mathcal{E}'$ which is an isomorphism of elliptic curves with $\Gamma[N]$-structure over $\overline{k(T)}$. Assume $\mathrm{char}(k) \neq 2, 3$ so they are isomorphic over a separable extension, L, of $k(T)$. If $\sigma \in \mathrm{Gal}(L/k(t))$, then we can consider $\psi = \varphi^{-1} \circ \varphi^\sigma : \mathcal{E} \to \mathcal{E}$. Now we need a lemma.

Lemma 2. *If E is an elliptic curve, $N \geq 3$, and $\psi \in \mathrm{Aut}(E)$ is trivial on $E[N]/(\pm 1)$, then $\psi = \pm 1$*

Proof: Since $\mathrm{Aut}(E) = \{\pm 1\}$ for $j \neq 0, 1728$, we only need to consider the two cases $j = 0, 1728$ and these can be done by direct calculation.

Now, our ψ is trivial on $\mathcal{E}[N]/(\pm 1)$, so $\psi = \pm 1$, and φ descends to $k(T)$. The second statement is similar and follows from the following lemma, whose proof is similar to that of the first lemma.

Lemma 3. *If E is an elliptic curve, and $\psi \in \mathrm{Aut}(E)$ is such that $\psi(P) = \pm P$ for some P of order $N \geq 5$, then $\psi = \pm 1$.*

Remark: $Y_0(N)$ is never a fine moduli space because an elliptic curve with j-invariant 0 or 1728 and $\Gamma_0[N]$ structure can still have automorphisms. For example, $[w]P = kP$ happens. If $E : y^2 = x^3 + 1$, $[w](x, y) = (wx, y)$, where

$w^3 = 1$, and $N \equiv 1 \bmod 3$, with N prime, then $[w]$ acts on $E[N]$ by a matrix having characteristic polynomial $x^2 + x + 1$.

March 9, 2010

Let $E : y^2 = x^3 + \frac{3t}{1728-t}x + \frac{2t}{1728-t}$ be an elliptic curve over $k(t)$, where k contains a primitive Nth root of unity ζ. We will now prove the claim made at the beginning of the notes regarding $\mathrm{Gal}(F_N^+/k(t))$.

Let F/E be an extension of function fields over k which is Galois with group G. Assume that k is algebraically closed in F. We have a corresponding map of curves $Y \to X$. Let v be a place of E with corresponding place w in F, and P be a point corresponding to v in X with the point $Q \in Y$ over it. Then we can define $G_w = \{\sigma \in G | w \circ \sigma = w\} = \{\sigma \in G | \sigma Q = Q\}$ $= \mathrm{Gal}(F_w/E_v) \subset G$. G_w is trivial if v is unramified.

Comment: If H is the subgroup of G generated by all the G_w, then F^H/E is unramified. If $E = k(t)$, then $k(t)$ has no unramified extensions, so $F^H = E$, i.e., $H = G$.

Now, we know that $F_N/k(t)$ is ramified only above 0, 1728, and ∞. So the strategy for the proof will be to identify the ramifications groups at 1728 and ∞. Ramification at ∞ gives $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$ ($\mathrm{ord}(T) = N$). Ramification at 1728 gives $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G$ ($\mathrm{ord}(S) = 4$). Finally, ramification at 0 gives ST (which has order 6).

Lemma 4. *S and T generate $SL_2(\mathbb{Z})/\{\pm I\}$.*

Proof: Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})/\{\pm I\}$. Without loss of generality, we may assume $c \geq 0$. Proceed by induction on c. Note $ad - bc = 1$. If $c = 0$, then $ad = 1$, so $a = d = \pm 1$. Hence, $\gamma = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} = \pm T^b$. The induction hypothesis is that all elements of $SL_2(\mathbb{Z})$ with lower left entry $\leq c$ are in $\langle S, T \rangle$. If $c > 0$, write $d = cq + r$, $0 \leq r < c$.

Then

$$\gamma T^{-q} = \begin{pmatrix} a & -aq + b \\ c & r \end{pmatrix}.$$

This implies that

$$\gamma T^{-q} S = \begin{pmatrix} -aq+b & -a \\ r & -c \end{pmatrix} \in \langle S, T \rangle$$

by the induction hypothesis, as $r < c$, so $\gamma \in \langle S, T \rangle$.

Lemma 5. *The reduction mod N, $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N)$, is surjective.*

Proof: Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/N)$, that is, $a, b, c, d \in \mathbb{Z}$ and $ad - bc \equiv 1 \bmod N$. So there is $m \in \mathbb{Z}$ so that $ad - bc - mN = 1$. Hence, c, d, and N are relatively prime. So there is $k \in \mathbb{Z}$ such that $(c, d + kN) = 1$ (Exercise). We can change d to $d + kN$ so without loss of generality, $(c, d) = 1$. Hence, there are $u, v \in \mathbb{Z}$ so that $ud - vc = -m$, and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+uN & b+vN \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z}/N)$. Then the determinant of this last matrix is $(a+uN)d-(b+vN)c = ad-bc+N(ud-vc) = 1+N(ud-vc+m) = 1$ soit belongs to $SL_2(\mathbb{Z})$ and the result is proved.

Now we consider the ramifications above ∞ and 1728.

Ramification above ∞: Use the Tate curve. $t = j(E) = q^{-1} + \sum c_n q^n$ so q is some power series in t and $k((t^{-1})) = k((q))$. Also $E(L) = L^*/q^{\mathbb{Z}}$ if L is a complete field extending $k((q))$, and u gives a point of order N if and only if $u^N \in q^{\mathbb{Z}}$. So

$$E[N] = \left\{ \zeta^a (q^{\frac{1}{N}})^b | 0 \le a, b \le N-1 \right\} \subset k((q^{\frac{1}{N}}))^*/q^{\mathbb{Z}},$$

where $q^{\frac{1}{N}}$ is some Nth root of q in $\overline{k((q))}$. So $(F_N)_w = k((q^{\frac{1}{N}}))$ if $w|\infty$ and

$$\mathrm{Gal}((F_N)_w/k((q))) = \mathrm{Gal}(k((q^{\frac{1}{N}}))/k((q))) = \mathrm{Gal}(k((q))(q^{\frac{1}{N}})/k((q))) = \mathbb{Z}/N$$

with generator σ, where $\sigma(q^{\frac{1}{N}}) = \zeta q^{\frac{1}{N}}$ and $\sigma(\zeta) = \zeta$. The points on $E[N]$ corresponding to $q^{\frac{1}{N}}$ and ζ form a basis of $E[N]$, so $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in this basis.

Ramification above 1728: We have the elliptic curve $y^2 = x^3 + \frac{3t}{1728-t}x + \frac{2t}{1728-t}$. Let $\lambda^4 = 1728 - t$. $u = 1728 - t$ is a local parameter

near 1728. Let $y = \frac{y_1}{\lambda^3}$ and $x = \frac{x_1}{\lambda^2}$. This gives us the curve with equation $y_1^2 = x_1^3 + \frac{3t\lambda^4}{1728-t}x_1 + \frac{2t\lambda^6}{1728-t} = x_1^3 + 3tx_1 + 2t\lambda^2$. At $\lambda = 0$, we get $y_1^2 = x_1^3 + 3(1728)x_1$, which is an elliptic curve with j-invariant 1728.

Now $\lambda^4 = u$ so $\mathrm{Gal}(k((\lambda))/k((u))) = \mathbb{Z}/4$, generated by $\sigma : \lambda \mapsto i\lambda$. If $(x, y) \in E[N]$, then $\sigma(y) = y$ so $\sigma(y_1) = i^3 y_1 = -iy_1$, and $\sigma(x) = x$ so $\sigma(x_1) = i^2 x_1 = -x_1$. That is, σ acts on E_{1728} by $[i] : (x_1, y_1) \mapsto (-x_1, -iy_1)$, (Note that i is in k, since it is assumed algebraically closed). Now, we can find $P_1 \in E[N]$ so that P_1 and $[i]P_1$ form a basis for $E[N]$. Now, $\sigma(P_1) = [i]P_1$ and $\sigma([i]P_1) = -P_1$ so $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z}/N)$ in this basis.

The bases for $E[N]$ that we used for ∞ and 1728 are actually the same so we do produce the matrices S, T in $SL_2(\mathbb{Z}/N)$, so we can conclude that the Galois group is $SL_2(\mathbb{Z}/N)/\{\pm 1\}$ from the above lemmas. Over $\mathbb{C}$ it is easy to see the bases are the same and indeed they both correspond to $1/N, \tau/N \in \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$. At infinity, $q = e^{2\pi i\tau}$ and at $1728, \tau = i$. We won't check that the bases are the same for arbitrary k.

Elliptic Curves

Felipe Voloch

March 30, 2010

$X_1(N) \to X_0(N)$

We consider here

$$X_1(N) \to X_0(N),$$

which we may choose to think of as

$$(E, P) \to (E, \langle P \rangle) \quad \text{or alternatively,} \quad X(N)/H_1 \to X(N)/H_2$$

where

$$H_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\} \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$$
$$H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = 1 \right\} \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$$

Note that $H_1 \trianglelefteq H_2$ and $H_2/H_1 \cong (\mathbb{Z}/N\mathbb{Z})^*/\pm 1$. $X_1(N)$ is acted on by

$$\langle d \rangle : X_1(N) \to X_1(N), \quad (E, P) \mapsto (E, dP).$$

The action of $\langle -1 \rangle$ is trivial, since -1 is an isomorphism of E sending P to $-P$. These $\langle \cdot \rangle$ are called the **diamond operators**.

Our previous calculations show that $X_1(N) \to X_0(N)$ is unramified above $j = \infty$. Ramification at (E, P) occurs if there exists some $d \in (\mathbb{Z}/N\mathbb{Z})^*/\pm 1$ with $d \neq \pm 1$ such that $(E, P) = (E, dP)$ as elliptic curves with level N structures—i.e., there exists some $\varphi \in \mathrm{Aut}(E)$ such that $\varphi(P) = dP$. If $\varphi = \pm 1$, then we already have $(E, P) = (E, -P)$, so $d = \pm 1$, which is excluded.

We need $\varphi \neq \pm 1$, so $j = 0$ or 1728. If $j = 1728$, then $\varphi \neq \pm 1$ implies $\varphi^2 = -1$. Assume N is prime. Then φ has characteristic polynomial $x^2 + 1$ when thought of as a linear operator over $\mathbb{Z}/N\mathbb{Z}$ (a field, by assumption). If $N \equiv 3 \mod 4$, then x^2+1 is irreducible over $\mathbb{Z}/N\mathbb{Z}$, so φ has no eigenspaces and there is no such d. If $N \equiv 1 \mod 4$, then $x^2 + 1$ factors $\mod N$ and φ has two eigenspaces. These correspond to ramification points.

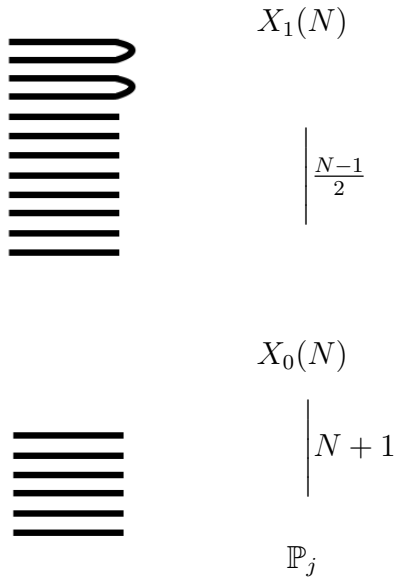


Figure 1: Ramification in the case $N = 5$.

There are $N+1$ points in $X_0(N)$ above $j = 1728$. Two of them ramify in $X_1(N)$ giving $(N-1)/4$ points with ramification index 2. The other $N-1$ split into $(N-1)/2$ pairs.

For $j = 0$, $\varphi \in \mathrm{Aut}(E)$, $\varphi \neq \pm 1$, so φ satisfies $\varphi^2 \pm \varphi + 1 = 0$. When $N \equiv 2 \mod 3$, these polynomials are irreducible, so no ramification. When $N \cong 1 \mod 3$, there is ramification. When $N = 3$, it's another story.

Equations for $X_1(N)$

Idea: Given (E, P), we want to embed E in $\mathbb{P}^2$ by a general Weierstrass equation

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

We will choose coordinates so that $P = (0, 0)$, which means $a_6 = 0$. We shall also require that the tangent at P, $T_P E$, is $y = 0$, which is possible when $2P \neq 0$ (here, we have assumed $N > 2$). This constraint forces $a_4 = 0$. Thus, we have an equation of the type

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2.$$

We can still change variables through the usual

$$x \mapsto \lambda^2 x, \quad y \mapsto \lambda^3 y$$

which will yield

$$a_1 \mapsto a_1/\lambda = a_1', \quad a_2 \mapsto a_2/\lambda^2 = a_2', \quad a_3 \mapsto a_3/\lambda^3 = a_3'.$$

We may then choose λ so that $a_3' = a_2'$, i.e. $\lambda = a_3/a_2$. Our ability to do this assumes both a_2 and a_3 are nonzero. (Had a_3 been zero, our curve would have been singular.) Now we have

$$E : y^2 + axy + by = x^3 + bx^2, \quad P = (0, 0).$$

When $y = 0$, we see that $x^3 + bx^2 = 0$, so $x = 0$ (a double root) or $x = -b$. Thus, we may compute

$$\begin{aligned} -2P &= (-b, 0), \\ 2P &= (-b, ab - b), \\ 3P &= (-a + 1, a - b - 1). \end{aligned}$$

If we assume $4P = 0$, this is equivalent to $2P = -2P$, meaning $(a - 1)b = 0$. Since $b \neq 0$, we force $a = 1$. Then

$$E : y^2 + xy + by = x^3 + bx^2$$

is the universal elliptic curve with point of order 4. $Y_1(4)$ is the b-line with some points excluded. $X_1(4) = \mathbb{P}^1_b$.

If we assume $5P = 0$, this is equivalent to $3P = -2P$, or $a - b = 1$ by examining coordinates. $Y_1(5)$ is the a-line, $X_1(5) = \mathbb{P}^1_a$, and the associated universal elliptic curve is

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

Similarly, $X_1(7) = \mathbb{P}^1_d$ with $a = 1 - d(d + 1), b = -d^2(d - 1)$.

April 1, 2010

Correspondences

Let X, Y be smooth projective curves over K. A **correspondence from X to Y** is a curve C together with a nonconstant map $f : C \to X \times Y$ such that $\pi_X \circ f$ and $\pi_Y \circ f$ are surjective, where $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ are the standard projection maps. A correspondence induces a map defined for $P \in X$ by

$$P \mapsto (\pi_Y \circ f)_*((\pi_X \circ f)^*(P)) = C(P).$$

$X \to Y^{(d)} = Y^d/S_d$, where $Y^{(d)}$ is the space parametrizing positive divisors of degree d on Y and $d = \deg(\pi_X \circ f)$.

In the diagram below, some values of the map are given by $P_1 \mapsto Q_1 + Q_2$ and $P_2 \mapsto 2Q_3$.

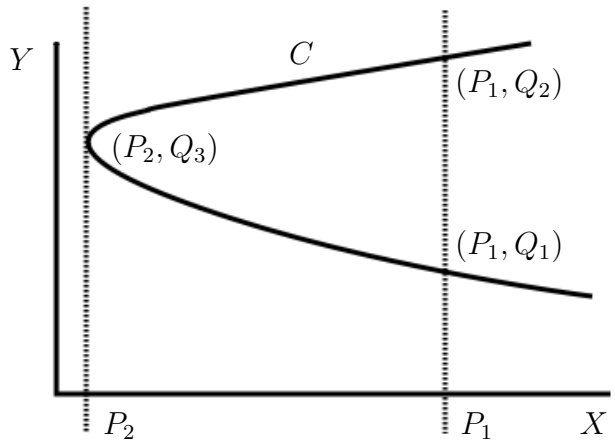


Figure 2: C as a curve in $X \times Y$.

Given a correspondence from X to Y, we get a correspondence from Y to X by

$$f : C \to X \times Y \to Y \times X, \quad (x, y) \mapsto (y, x).$$

This is called the **dual correspondence**.

The **Jacobian of** X, denoted $Jac(X)$, is the group of divisors of degree 0 modulo principal divisors. We will not show this, but $\mathrm{Jac}(X)$ is an abelian variety of dimension $g = \mathrm{genus}(X)$.

Fix $P_0 \in X$, $Q_0 \in Y$, and a correspondence C from X to Y. We can define

$$\varphi_C : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$$

by linearly extending the map

$$P - P_0 \mapsto [C(P) - dQ_0].$$

This means that if $\sum_P n_P = 0$,

$$\varphi_C \left(\sum_P n_P P \right) = \sum_P n_P \varphi_C(P - P_0) = \sum_P n_P C(P).$$

The correspondence C from X to Y in this way gives rise to the homomorphism $\varphi_C : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$, which is independent of the choices of P_0, Q_0. Conversely, given a nonconstant homomorphism $\varphi : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$, we want to define a correspondence C from X to Y. If P is generic on X, $\varphi(P - P_0) = D_P - gQ_0$, where D_P is effective of degree g. The locus of D_P as P varies in X describes a curve in $X \times Y$.

More precisely, a correspondence is a linear equivalence class of divisors in $X \times Y$.

Composition of Correspondences

Let C be a correspondence from X to Y and D a correspondence from Y to Z. Then the fiber product $C \times_Y D$ is a correspondence from X to Z, where $C \times_Y D(P) = \sum_Q n_Q D(Q)$ if $C(P) = \sum_Q n_Q Q$. It can be shown that $\varphi_{C \times_Y D} = \varphi_D \circ \varphi_C$.

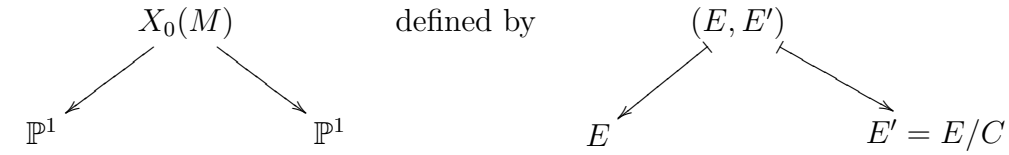
If $X = Y$, then the correspondences modulo linear equivalence form a ring (multiplication is given by composition and addition is defined by $C_1(P) + C_2(P) = (C_1 \cup C_2)(P)$) corresponding to $\mathrm{End}(\mathrm{Jac}(X))$.

Hecke Operators

Recall that

$$\begin{aligned} X_0(N) &= \{(E, E', \varphi) \,:\, \varphi : E \to E' \text{ cyclic of degree } N\} \\ &= \{(E, C) \,:\, |C| = N \text{ cyclic}\}. \end{aligned}$$

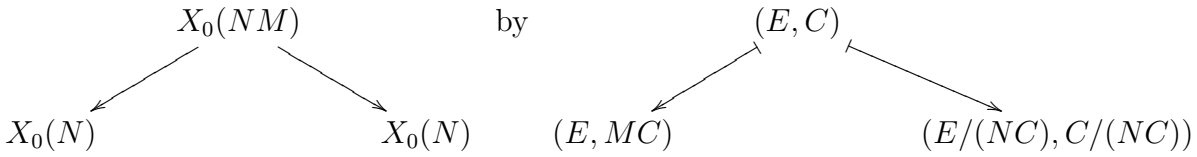
Then we may think of $X_0(M)$ as a correspondence from $\mathbb{P}^1$ to $\mathbb{P}^1$ (i.e. a curve in $\mathbb{P}^1 \times \mathbb{P}^1$):



If we take $(N, M) = 1$, then we have

$$X_0(NM) = \{(E, C) \,:\, E \text{ elliptic curve}, |C| = NM \text{ cyclic}\}.$$

We can write $C = C_1 \times C_2$ with $|C_1| = N$, $|C_2| = M$, $C_1 = MC$, $C_2 = NC$, $|C/C_2| = N$. The associated correspondence is then

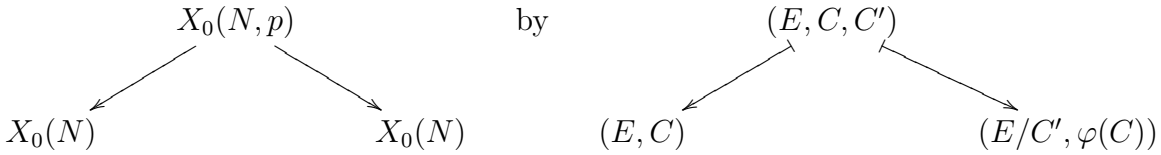


This defines a correspondence T_M from $X_0(N)$ to itself.

For p prime, $X_0(N, p)$ is the moduli space of triples (E, C, C') such that C is cyclic of order N, C' is cyclic of order p, and $C \cap C' = \{0\}$. When p does not divide N, $X_0(N, p) = X_0(Np)$ by the map $(E, C, C') \mapsto (E, C \oplus C')$. $X_0(N, p)$ can be viewed as $X(Np)/H$ where

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,:\, b \equiv 0 \mod N,\, c \equiv 0 \mod p \right\} \subset SL_2(\mathbb{Z}/Np).$$

Constructing for $\varphi : E \to E/C'$

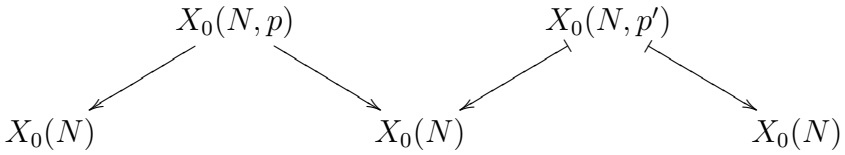


we have defined a correspondence T_p from $X_0(N)$ to itself.

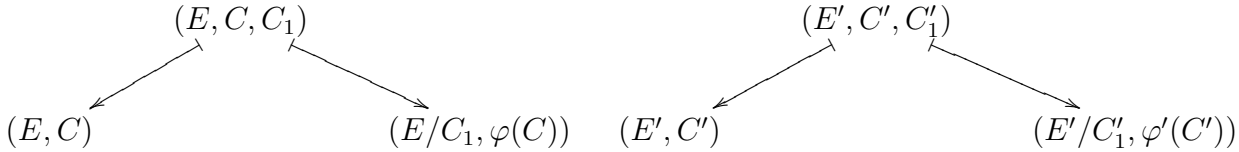
We have thus defined correspondences T_M and T_p from $X_0(N)$ to itself when $(M, N) = 1$ and when p prime. We can consider the subring of $\mathrm{End}(\mathrm{Jac}(X_0(N)))$ generated by the T_p, p prime.

Proposition: If p, p' are distinct primes, then $T_p T_{p'} = T_{p'} T_p$ as correspondences on $X_0(N)$. These furthermore equal $T_{pp'}$ if $(pp', N) = 1$.

Proof: We construct the following correspondences:



defined by



Here, $|C| = N, |C_1| = p, C \cap C_1 = \{0\}$. We then observe that

$$T_p((E,C)) = \sum_{\substack{|C_1|=p \\ C_1 \cap C = \{0\}}} (E/C, \varphi(C)),$$

so

$$T_{p'} T_p((E,C)) = \sum_{\substack{C_1 \subseteq E \\ |C_1|=p \\ C_1 \cap C = \{0\}}} \sum_{\substack{C_1' \subseteq E/C_1 \\ |C_1'|=p' \\ C_1' \cap \varphi(C) = \{0\}}} ((E/C_1)/C_1', \varphi'(\varphi(C))).$$

There exists a unique $C_1 \subseteq E$ of order p such that $\varphi\big|_{C_2}$ is an isomorphism onto C_1'. $\varphi^{-1}(C_1')$ is a group of order pp', so it has a subgroup C_2 of order p'. $\varphi^{-1}(C_1')/C_2$ has order p and $(E/C_2)/C_2' \cong (E/C_1)/C_1' \cong E/\varphi'(C_1')$. This relation can then be used to identify the terms in the above sum for $T_{p'} T_p$ and the corresponding sum for $T_p T_{p'}$. ■

Corollary: If M, M', N are pairwise relatively prime, then it follows that $T_M T_{M'} = T_{M'} T_M = T_{MM'}$.

ELLIPTIC CURVES, MODULAR CURVES, AND MODULAR FORMS

4/6/10

We begin with a computation involving the Hecke operator T_p, p a prime. We have, for an elliptic curve E (suppressing the level structure from the notation),

$$T_pT_p(E) = T_p\left(\sum_{C\leq E,\#E=p} E/C\right) = \sum_{\substack{C'\leq E/C\\ |C'|=p}}\sum_{\substack{C\leq E\\ |C|=p}} (E/C)/C'.$$

If C is a subgroup of E of order p, and C' a subgroup of E/C of order p, then we have a map $\varphi : E \to E/C \to (E/C)/C'$, the composite of the canonical maps. Then φ has degree p^2 (being the composite of two maps of degree p), so $|\ker\varphi| = p^2$, and $\ker\varphi$ is either cyclic of order p^2 or isomorphic to $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. In the latter case we have $\ker\varphi = E[p]$, the p-torsion of E (we're assuming throughout that p is prime to the characteristic of the field of definition of our elliptic curve); we then have (for a general elliptic curve) $\varphi = [p]$, the multiplication-by-p map. Putting this together, and considering both possibilities, we see that the above sum has the form

$$\sum_{\substack{D\leq E,\\ D\simeq\mathbb{Z}/p^2\mathbb{Z}}} E/D + kE,$$

where k is a constant corresponding to the number of times we have $\ker\varphi = E[p]$. But given a subgroup C of E of order p, to have $\varphi = [p]$, we must have $C' = \ker\varphi/C$. This gives $k = p+1$, so that

$$T_pT_p(E) = T_{p^2}(E) + (p+1)E,$$

hence $T_pT_p = T_{p^2} + (p+1)I$, where I is the identity. Note that, in other sources, T_{p^2} is defined to be our T_{p^2} plus the identity, so that, if we denote this modified operator by $\tilde{T}_{p^2}$, the formula becomes $T_pT_p = \tilde{T}_{p^2} + pI$. In general, using $\tilde{}$ to denote the modified Hecke

operators found elsewhere, one can show that

$$\tilde{T}_n \tilde{T}_m = \sum_{d|(m,n)} d\tilde{T}_{nm/d^2},$$

which, in particular, implies that $\tilde{T}_n \tilde{T}_m = \tilde{T}_m \tilde{T}_n$ when n and m are relatively prime. That is, when appropriately defined, the Hecke operators corresponding to relatively prime integers commute.

We now define the *Hecke algebra*, $\mathbb{T}$, to be $\mathbb{Z}[T_p]$, the ring of polynomials over $\mathbb{Z}$ in infinitely many indeterminates T_p, one for each prime p. Assuming we are in characteristic zero, for each N, because the Hecke operators can be viewed as endomorphisms of the modular Jacobian $J_0(N) = \mathrm{Jac}(X_0(N))$, we obtain a ring homomorphism $\mathbb{T} \to \mathrm{End}(J_0(N))$. We want to decompose the abelian variety $J_0(N)$ into factors using the image of the Hecke algebra $\mathbb{T}$ under this homomorphism.

We now pause to give basic definitions relating to abelian varieties. An *abelian variety* over a field K is a smooth projective group variety over K (or if you prefer scheme-theoretic language, a proper, geometrically integral K-group scheme). One can prove that with this definition, all abelian varieties are commutative as group varieties. To any smooth projective curve C over K of genus g, one can canonically associate a g-dimensional abelian variety $\mathrm{Jac}(C)$, the *Jacobian variety* of C. If A and B are abelian varieties, an isogeny $\varphi : A \to B$ is a non-constant, surjective morphism with finite kernel; if there exists an isogeny $\varphi : A \to B$, A and B are said to be *isogenous*. An abelian variety is *simple* if it has no proper, non-trivial abelian subvarieties. A result known as Poincaré's complete irreducibility theorem states that every abelian variety is isogenous to a product of simple abelian varieties, and that these factors are unique up to isogeny. If A is an abelian variety of dimension g defined over $\mathbb{C}$, then the group of $\mathbb{C}$-points $A(\mathbb{C})$ is a compact, complex, connected Lie group of dimension g, which necessarily has the form $\mathbb{C}^g/\Lambda$, where Λ is a lattice in $\mathbb{C}^g$ (a discrete, co-compact subgroup of $\mathbb{C}^g$). Note that the tangent space to the identity of $A(\mathbb{C})$ is $\mathbb{C}^g$.

Now we return to the Hecke algebra $\mathbb{T}$, which acts on $J_0(N)$ via the aforementioned ring map. $\mathbb{T}$ also acts on $T_{\mathcal{O}}J_0(N)$, the tangent space to the identity of $J_0(N)$. It is a fact that the abelian variety $J_0(N)$ is "square-free" in the sense that when it is factored into a product of simple abelian varieties, the factors are pairwise non-isogenous. Let $\mathbb{I}$ be an ideal of the image of $\mathbb{T}$ in $\mathrm{End}(J_0(N))$. Then $J_0(N)/\mathbb{I}J_0(N)$ is an abelian variety. Suppose that V is an eigenspace for the action of $\mathbb{T}$ on $T_{\mathcal{O}}J_0(N)$, and set $\mathbb{I}_V$ equal to the ideal generated by $T_p - a_p$, where p ranges over all prime and V is an a_p-eigenspace for T_p. Note that, a priori, it is only clear that $a_p \in \mathbb{C}$. We have the following theorem.

Theorem. *If V is an eigenspace for the action of $\mathbb{T}$ on $T_{\mathcal{O}}J_0(N)$, then the eigenvalues a_p are algebraic integers, and if $F_V = \mathbb{Q}(\{a_p : p \text{ prime }\})$, then F_V is a finite extension of $\mathbb{Q}$. In fact, $[F_V : \mathbb{Q}]$ is equal to the dimension of the abelian variety $J_0(N)/\mathbb{I}_V J_0(N)$.*

Note that if V is as above, then T_p acts as multiplication by a_p on V. Viewing V as a subspace of $\mathbb{C}^g$, we can map V to $\mathbb{C}^g/\Lambda$ (the complex points of $J_0(N)$), and we define A_V to be the abelian variety that is the image of this map. The case of interest for us is when V is one-dimensional. In this case, the a_p are actually rational integers, so by the above theorem, $J_0(N)/\mathbb{I}_V J_0(N)$ is an elliptic curve E_V. It is a theorem that E_V is in fact defined over $\mathbb{Q}$. Conversely, if $E/\mathbb{Q}$ is an elliptic curve defined over $\mathbb{Q}$ that is also a quotient (equivalently a factor) of $J_0(N)$, then because $J_0(N)$ is "square-free," E can only appear once (up to isogeny) as a factor of $J_0(N)$, so we must have $T_p(E) = E$ or $T_p(E) = 0$. It follows that in this case, $E = E_V$ for some eigenspace V for the action of $\mathbb{T}$. An elliptic curve defined over $\mathbb{Q}$ that is a quotient of $J_0(N)$ for some N is said to be *modular*. This leads us to the celebrated

Taniyama-Shimura-Weil Conjecture. *Every elliptic curve defined over $\mathbb{Q}$ is modular.*

We now know, thanks to the work of C. Breuil, B. Conrad, F. Diamond, R. Taylor, and A. Wiles, that the above conjecture is in fact true (and the result is now sometimes referred to as the modularity theorem). Note that we have defined an elliptic curve E over $\mathbb{Q}$ to be modular if it is a quotient of $J_0(N)$ for some N. In fact, because a curve maps canonically to its Jacobian, this is equivalent to the existence of a non-constant map $X_0(N) \to E$ for

some N over $\mathbb{C}$.

4/8/10

Recall that an elliptic curve $E/\mathbb{Q}$ is *modular* if it is a factor of $J_0(N) = \mathrm{Jac}(X_0(N))$ for some N. In fact, we have the following string of equivalences:

(1) E is modular;
(2) there exists some N and a non-constant map $X_0(N) \to E$ over $\mathbb{C}$;
(3) there exists some N and a non-constant map $X_0(N) \to E$ over $\mathbb{Q}$;
(4) the L-function of E has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating $L(s, E)$ and $L(2 - s, E)$;
(5) there exists a prime ℓ and some N such that $T_\ell E$ is a factor of $T_\ell J_0(N)$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

The equivalence of (1) and (2) is essentially just a property of the Jacobian of a curve. In the last property, $T_\ell E$ is the ℓ-adic Tate module of E. In general, if A is an abelian variety over a field K and ℓ is a prime different from the characteristic of K, $T_\ell A$ is defined to be the projective limit $\varprojlim A[\ell^n]$ of ℓ-power torsion groups taken with respect to the obvious maps. The ℓ-adic Tate module of A is a free $\mathbb{Z}_\ell$-module of rank $2 \dim A$: $T_\ell A \simeq \mathbb{Z}_\ell^{2 \dim A}$ as $\mathbb{Z}_\ell$-modules. The equivalence of (1) and (5) is a consequence of Faltings' isogeny theorem, which states that for abelian varieties A and B over a number field K, $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \simeq \mathrm{Hom}_{G_K}(T_\ell A, T_\ell B)$, where $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is the absolute Galois group of K.

One approach to the canonical mapping of a curve to its Jacobian (over the complex numbers) involving differentials is as follows. Given a smooth projective curve X of genus g, suppose that $\omega_1, \ldots, \omega_g$ give a basis for the vector space of holomorphic differentials on X. We can think of $\mathrm{Jac}(X)$ as $\mathbb{C}^g/\Lambda$, where Λ is the period lattice of X: $\Lambda = \{(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g) : \gamma \in \pi_1(X)\}$. The map from X to $\mathrm{Jac}(X)$ can then be described as $P \mapsto (\int_{P_0}^P \omega_1, \ldots, \int_{P_0}^P \omega_g)$ (here $P_0 \in X$ is a fixed point).

Let $E/\mathbb{Q}$ be an elliptic curve and $\varphi : X_0(N) \to E$ a non-constant map. If ω is an invariant differential on E, then $\omega' = \varphi^*\omega$ is a holomorphic differential on $X_0(N)$. If E corresponds to a Hecke eigenspace V, i.e., $E = J_0(N)/\mathbb{I}_V J_0(N)$, where $\mathbb{I}_V$ is the ideal generated by $T_p - a_p$, where p is a prime and a_p the associated eigenvalue of T_p, then $T_pE \subseteq E$, T_p acts on E as a_p, and $T_p^*\omega' = a_p\omega'$.

We now move to the introduction of modular forms. Over $\mathbb{C}$, $X_0(N)$ is the compactification of $\mathfrak{h}/\Gamma_0(N)$ (here $\mathfrak{h}$ is the complex upper half-plane). A differential form on $\mathfrak{h}/\Gamma_0(N)$ is an expression $f(\tau)\,\mathrm{d}\,\tau$ invariant under $\Gamma_0(N)$. What exactly does $\Gamma_0(N)$-invariance mean in this case? We require that for each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$,

$$f\left(\frac{a\tau+b}{c\tau+d}\right)\mathrm{d}\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau)\,\mathrm{d}\,\tau,$$

which means

$$f\left(\frac{a\tau+b}{c\tau+d}\right)\frac{(c\tau+d)a-(a\tau+b)c}{(c\tau+d)^2}\,\mathrm{d}\,\tau = f(\tau)\,\mathrm{d}\,\tau.$$

Since $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $ad - bc = 1$, and the above relation becomes

$$f\left(\frac{a\tau+b}{c\tau+d}\right)\frac{\mathrm{d}\,\tau}{(c\tau+d)^2} = f(\tau)\,\mathrm{d}\,\tau,$$

or $f(\gamma\tau)\,\mathrm{d}\,\tau = (c\tau+d)^2 f(\tau)\,\mathrm{d}\,\tau$, which forces $f(\gamma\tau) = (c\tau+d)^2 f(\tau)$. This leads to our first

Provisional Definition. A complex modular form of weight k for $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ (if Γ is one of $\Gamma(N), \Gamma_0(N), \Gamma_1(N)$, N is the level of the modular form) is a holomorphic function $f : \mathfrak{h} \to \mathbb{C}$ with $f(\gamma\tau) = (c\tau+d)^k f(\tau)$ for each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, and such that $f(q)$ is holomorphic, where, as usual $q = \exp(2\pi i\tau)$.

The next provisional definition is also inspired by the preceding computation.

Provisional Definition. A modular form of weight 2 for $\Gamma_0(N)$ (similarly for $\Gamma_1(N), \Gamma(N)$) over a field K is a differential form on $X_0(N)$ with at most simple poles at the cusps and no others.

Consider the case when $K = \mathbb{C}$, and $f(\tau)\,\mathrm{d}\,\tau$ is a differential on $X_0(N)$, $q = \exp(2\pi i\tau)$. We then have $q^{-1}\,\mathrm{d}\,q = 2\pi i\,\mathrm{d}\,\tau$, so

$$f(\tau)\,\mathrm{d}\,\tau = \frac{f(q)\,\mathrm{d}\,q}{2\pi i q},$$

and $(2\pi i q)^{-1} f(q)\,\mathrm{d}\,q$ has a simple pole at $q = 0$ if and only if $f(q)$ is holomorphic for $q = 0$. Thus our second provisional definition generalizes our first with $k = 2$.

A modular form that vanishes at the cusps is called a *cusp form*. A modular form f is an *eigenform* for the Hecke algebra if $T_p f = a_p f$ for all primes p (and some a_p). The modular forms for $\Gamma_0(N)$ form a finite-dimensional vector space $\mathcal{M}_0(k, N)$ with the cusp forms forming a subspace $\mathcal{S}_0(k, N)$. The Hecke algebra acts on these spaces and the eigenforms as defined above are eigenvectors for this action (simultaneous eigenvectors for all of the Hecke operators).

Suppose that X is a fine moduli space of elliptic curves with some level structure (e.g. $X = X_1(N), X(N)$, but *not* $X_0(N)$). Then there exists a universal elliptic curve $\mathcal{E} \to X$ equipped with a section $\mathcal{O} : X \to \mathcal{E}$. The fibers of $\mathcal{E} \to X$ are elliptic curves in the usual sense, and for each fiber, we get a one-dimensional vector space of holomorphic differentials. So we have a 1-parameter family of one-dimensional vector spaces. Set $\underline{\omega} = \mathcal{O}^*\Omega^1_{\mathcal{E}/X}$. This is a line bundle on X. This brings us to the

Official Definition. A modular form of weight k on X is a global section of $\underline{\omega}^{\otimes k}$, i.e., an element of $H^0(X, \underline{\omega}^{\otimes k})$.

The content of the following theorem is (essentially) that our official definition generalizes our provisional one(s).

Theorem. *(Kodaira-Spencer)* $\underline{\omega}^{\otimes 2} = \Omega^1_X(\mathit{cusps})$.

An equivalent formulation of the official definition is as follows. A modular form f of weight k over a field K (for some level structure) is a rule assigning (for any K-algebra R) to each triple (E, C, ω), where R is a K-algebra, E an elliptic curve over R, C some level structure on E, and ω an invariant differential on E, an element $f(E, C, \omega) \in R$ such that

(1) f is functorial in the obvious sense;

(2) $f(E, C, \lambda\omega) = \lambda^{-k} f(E, C, \omega)$ for $\lambda \in K^\times$;

(3) $f(\mathrm{Tate}_q, C, \mathrm{d}\, u/u) \in K[[q]]$, where Tate_q is the Tate curve $K((q))^\times/q^{\mathbb{Z}}$ (this condition corresponds to holomorphicity at the cusps).

Modular forms of weight k for $X_0(N)$ are the modular forms of weight k for $X_1(N)$ that are invariant under the diamond operators. Recall that we have a Galois covering $X_1(N) \to X_0(N)$, $(E, P) \to (E, \langle P \rangle)$, with Galois group $G = (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, and for d prime to N, the diamond operator on $X_1(N)$ sends (E, P) to (E, dP). More explicitly, the modular forms of weight k for $X_1(N)$ are the global sections $H^0(X_1(N), \underline{\omega}^{\otimes k})$, and G acts on this vector space as the diamond operators. Because G is finite abelian, we obtain a decomposition $H^0(X_1(N), \underline{\omega}^{\otimes k}) = \bigoplus_{\epsilon \in \hat{G}} H^0(X_1(N), \underline{\omega}^{\otimes k})^{(\epsilon)}$, where $\hat{G}$ is the dual group of G (its group of characters). The weight k modular forms for $X_0(N)$ are the elements of the summand corresponding to ϵ_0, the trivial character. Elements of the summands for ϵ a non-trivial character are called *modular forms with character* ϵ. In the complex analytic picture, such a modular form is a modular form f in the usual sense except that its transformation rule is "twisted by ϵ," i.e.,

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = \epsilon(d)(c\tau + d)^k f(\tau)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \supseteq \Gamma_1(N)$.

1 Elliptic Curves Notes May 4, 2010

Lemma 1. *Let $E/\mathbb{Q}$ be semistable. Let l and p be distinct primes with $l \neq 2, 3$. Suppose E has multiplicative reduction at l and*

$$v_l(\Delta) \equiv 0 \mod p$$

Then $\mathbb{Q}(E[p])/\mathbb{Q}$ is unramified at l.

Proof. Let E be given by $y^2 = x^3 + ax + b$. $\Delta = 4a^3 + 27b^2$, $j = 1728 \cdot (4a^3/\Delta)$. Multiplicative reduction implies that $\Delta \equiv 0 \mod l$. $a \neq 0 \mod l$, because $\Delta \equiv a \equiv 0 \mod l$ implies that $b \equiv 0 \mod l$, which implies additive reduction.

So,

$$v_l(j) = -v_l(\Delta) \equiv 0 \mod p$$

Since E has multiplicative reduction, E has a split multiplicative reduction on a field k, unramified at l. Over k_l,E is a Tate curve with parameter $q \in k_l^*$ (Tate curve with parameter q: $k_l^*/q^{\mathbb{Z}}$). We have

$$j = \frac{1}{q} + 744 + \cdots$$

So,

$$v_l(q) \equiv -v_l(j) \equiv 0 \mod p.$$

Thus,

$$k_l(E[p]) = k_l(\mu_p, q^{1/p}),$$

but $v_l(q) \equiv 0 \mod p$, so $k_l(\mu, q^{1/p})$ is unramified. □

This lemma implies that if $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $a^p + b^p + c^p = 0$, then by letting E be the curve $y^2 = x(x-a^p)(x+b^p)$ (the Frey curve E_{abc}), we have that the conductor of the representation is $E[p]$ is $N = 1$, i.e. $\mathbb{Q}(E[p])/\mathbb{Q}$ is unramified outside of p.

Ribet proved that if $E[p]$, for any elliptic curve E, is modular, then it is modular of level equaling the conductor of the representation. So, if $E_{abc}[p]$ is modular, then it must be modular of level 1. There are no such things. So, Frey + Ribet implies that $E_{abc}[p]$ is not modular.

Suppose that E is an elliptic curve with either good or multiplicative reduction and all primes (e.g. E_{abc}). Then $E[3]$ is modular by a theorem of Langlands and Tunnell. This is because $E[3]$ gives a representation

$$G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_3).$$

(Here, $G_{\mathbb{Q}}$ is the absolute Galois group of the rationals. Note: $GL_2(\mathbb{F}_3)$ is a group of order 48.) There is an embedding

$$GL_2(\mathbb{F}_3) \hookrightarrow GL_2(\mathbb{C}).$$

So, we get $G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ with solvable image and the theorem of Langlands and Tunnell shows "automorphy" of this representation, which implies modularity.

Wiles proved, by induction on n, that $E[3^n]$ is modular, for all n. He studies deformations of Galois representations. If

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_q),$$

then a deformation is a representation

$$\tilde{\rho} : G_{\mathbb{Q}} \longrightarrow GL_2(R)$$

such that there exists an ideal $I \subseteq R$ with $R/I = \mathbb{F}_q$ and $\tilde{\rho} = \rho \mod I$. There is a ring R which is the "universal deformation ring" of a representation, with the properties you might expect. To prove modularity, you need to prove that this R is the Hecke algebra. (This is often called an $R = \mathbb{T}$ theorem, and is proved using commutative algebra and Galois cohomology).

Wiles concludes that $T_3E = \varprojlim E[3^n]$ is modular. Since T_3E is modular, E is modular. (i.e. T_3E is a factor of $T_3J_0(N)$ for some N, as a $G_{\mathbb{Q}}$-module). This follows from a result of Falting (Tate's isogeny conjecture). It is part of his proof of Mordell's conjecture.

2 Elliptic Curves Notes May 4, 2010

Let $q = p^m$. Suppose

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_q)$$

is continuous. So, $\bar{\mathbb{Q}}^{\ker \rho} = k$ is a number field, and

$$Gal(k/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{F}_q).$$

Let ρ have conductor N_ρ, then $l | N_\rho$ if and only if $l \neq p$ and l is ramified in $k/\mathbb{Q}$.

Suppose $l \nmid pN_\rho$, so l is unramified in k. One can consider Frob(l) which is a conjugacy class in Gal($k/\mathbb{Q}$). So, det(Frob(l)) and Tr(Frob(l)) are well defined elements of $\mathbb{F}_q$.

We know that modular forms of weight 2 which are eigenforms of the Hecke algebra correspond to factors of the Jacobian of modular forms. Hence, they give rise to Galois representations of the torsion of those factors. There is a way of getting mod p representations from mod p modular forms of any weight. Serre's conjecture predicts that all "odd" two dimensional representations mod p of $G_{\mathbb{Q}}$ arise this way. Khare and Winterberger proved Serre's conjecture in 2008.

Definition. ρ is *modular* if there exists a modular cusp form f of weight k and level N ($p \nmid N$) over $\mathbb{F}_q$ for $X_1(N)$, which is an eigenform for the Hecke operator and the diamond operators such that:

$$\begin{aligned} \mathrm{Tr}(\rho(\mathrm{Frob}(l))) &= a_l \\ \det(\rho(\mathrm{Frob}(l))) &= \varepsilon(l) l^{k-l} \mod p. \end{aligned}$$

Recall that,

$$f \in H^0(X_1(N))/\mathbb{F}_q, \omega^{\otimes k}) \qquad \text{(vanishing at the cusps)}$$

(here $\omega = \mathcal{O}^* \Omega^1_{E/X_1(N)}$ is a sheaf on $X_1(N)$, where $\mathcal{O}$ is the zero section of the universal $E/X_1(N)$.) then

$$T_l f = a_l f$$

for all $l \nmid pN$, and

$$\langle d \rangle f = \varepsilon(d) f$$

for all d in $(\mathbb{Z}/N)^*$ (again $l \nmid pN$).

If g is a modular form for $X_1(N)$ of weight 2, level N, in characteristic 0 which is an eigenform for the Hecke algebra, then g gives an abelian subvariety of $J_1(N)$; call it A_g. So, $A_g[p]$ gives a Galois representation which is modular, in the above sense, with $f \equiv g \mod p$.

Theorem 2 (Deligne-Carayol)**.** *For any modular form f satisfying the conditions of the definition, there exists a galois representation which is modular with f.*

Eichler-Shimura relation: $T_p \equiv F + F' \mod p$, as correspondences on $X_0(N)$. In $X_1(N)$, something similar happens:

$$T_p \equiv F + \langle p \rangle F' \mod p.$$

(F is the Frobenius on $X_1(N)$ modulo p.)

A modular form g of weight 2 in $X_1(N_p)$ which is an eigenform for the diamond and Hecke operators gives an abelian variety $A_g \subseteq J_1(N_p)$. $A_g[p]$ has a determinant that looks like $\varepsilon(l)l^{k-1} \mod p$, for some k. Morally, a modular form of weight 2 in $X_1(Np)$ modulo p looks like a modular form of some weight k in $X_1(N)$.

To prove the theorem: given f in $X_1(N)/\mathbb{F}_q$, find g in $X_1(Np)/\bar{\mathbb{Q}}$ such that $g \equiv f \mod p$. Use g to construct p.

Theorem 3 (Khare - Winterberger, formerly the Serre conjecture)**.** *Every Galois representation $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_q)$ which is odd ($det(\rho(complex\ conjugation)) = -1$) and irreducible is modular.*

There is a strong version of the theorem which predicts N, k, ε from ρ. It was proven earlier that the weak version implies the strong version.

Serre + Ribet implies modularity (without lifting).

For all p, look at $E[p]$. By Serre, $E[p]$ is modular, so we get a modular form f_p modulo p, of level N and weight 2. For each f_p, we obtain a modular form g_p over $\mathbb{Q}$ of level N and weight 2, with $g_p \equiv f_p \mod p$. As g_p is one of the eigenforms for the Hecke algebra, g_p lies in a finite set, so $g_p = g$ for some g and infinitely many p.

($T_l g_p = a_l g_p$. $a_l = l + 1 - E(\mathbb{F}_q)$, is independent of p. So, $T_l g_p = a_l g_p$ which implies $L(E, p) = L(g, p)$ which implies F is modular.)