

# Real-p-Adic Analysis

## Lecture 1

Robert F. Coleman

### Elliptic Curves

#### Weierstrass Parametrization

Suppose  $\alpha, \beta \in \mathbf{C}$  and independent over  $\mathbf{R}$ . Then  $E := \mathbf{C}/(\alpha\mathbf{Z} + \beta\mathbf{Z})$  is a genus one Riemann surface. Weierstrass realized that this is also an algebraic curve, in fact, every smooth genus 1 algebraic curve over  $\mathbf{C}$  looks like this.

Suppose  $\frac{\beta}{\alpha} = \tau \in \mathcal{H}$ . Then  $E \cong \mathbf{C}^*/q^{\mathbf{Z}}$  where  $q = \exp(2\pi i\tau)$ . Then if  $F$  is a function on  $\mathbf{C}^*$  and

$$F(qu) = F(z)$$

$F$  is a function on  $E$ , which I'm now calling  $E_q$ . We better allow poles.

Let

$$X_q(u) = \sum_{n \in \mathbf{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2s_1(q) \quad \text{and} \quad Y_q(u) = \sum_{n \in \mathbf{Z}} \frac{q^n u}{(1 - q^n u)^3} + s_1(q)$$

where

$$s_k(q) = \sum_{n=1}^{\infty} \frac{n^k q^n}{1 - q^n}.$$

Then  $(X_q(u), Y_q(u))$  is a point on the completion  $C_{c,d}$  of the algebraic curve

$$y^2 + xy = x^3 + cx + d,$$

where  $c = a_4(q) = -s_3(q)$  and  $d = a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}$ . In fact, we get a holomorphism  $E_q \rightarrow C_{c,d}(\mathbf{C})$ .

## Tate Curves

Now suppose  $K$  is a finite extension of  $\mathbf{Q}_p$ ,  $|p| = p^{-1}$ . Then when  $|q| < 1$ , all the above series converge on  $(K^{alg})^*$ . So do we get an “analytic” isomorphism  $(K^{alg})^*/q^{\mathbf{Z}}$  onto  $C_{c,d}(K^{alg})$ , where  $c = a_4(q)$  and  $d = a_6(q)$ . Look at [Sil. V.4] Note that

$$j(C_{c,d}) = q^{-1} + 744 + 196884q + \dots$$

In particular, if an elliptic curve can be parametrized this way its  $j$ -invariant is not an integer. This parametrization is Galois equivariant.

**Theorem.** (Tate) *Let  $E$  be an elliptic curve over  $K$  with  $|j| > 1$ . Then there is a unique  $q \in K^*$ ,  $|q| < 1$  such that over a quadratic extension of  $K$ ,  $E \cong \mathbf{G}_m/q^{\mathbf{Z}}$ .*

## CM-curves

**Theorem.** *Suppose  $A$  is an elliptic curve over a number field  $K \subset \mathbf{C}$  and  $\text{End}_K(A) \neq \mathbf{Z}$ . Then  $j(A)$  is an algebraic integer.*

*Proof.* (Due to Serre.) Suppose  $\psi$  is an endomorphism,  $\psi \notin \mathbf{Z}$ . Then using Weierstrass and Cayley-Hamilton we see there exist  $b, c \in \mathbf{Z}$  such that

$$\psi^2 + b\psi + c = 0,$$

moreover  $x^2 + bx + c$  has distinct non-real roots. Let  $L$  be its splitting field in  $\mathbf{C}$  over  $K$ .

Suppose  $\pi$  is a prime of  $L$  such that  $|j(A)|_\pi > 1$ .

Now let  $\ell$  be a prime which splits completely in  $L$ ,  $\ell \nmid v_\pi(j(A))$ . Then the matrix for  $\psi$  acting on  $A[\ell]$  is diagonalizable with distinct roots. Fix  $\ell$ .

Now we pass to  $L_\pi$ . Claim: There exists a  $\sigma$  in the inertia group of  $L_\pi^{alg}/L$  such that the action of  $\sigma$  on  $A[\ell]$  is unipotent and not trivial. We can assume  $A = E_q$  for some  $q \in L_\pi^*$  and  $A[\ell](L_\pi^{alg}) \subset A(L_\pi)$ .

Then  $A[\ell](L_\pi^{alg})$  is the image of  $\{x \in L_\pi^{alg} : x^\ell \in q^{\mathbf{Z}}\}$ .