

# Diophantine Geometry Notes

taken by Grant Lakeland

March 6, 2008

Let  $K$  be a global field.  $A/K$  will be an abelian variety of dimension  $n$ ,  $M_K$  the set of places of  $K$ , and  $S$  the set of places of bad reduction and archimedean places.

Suppose  $v$  is a non-archimedean place, with corresponding absolute value  $|\cdot|_v$  and completion  $K_v$ . Let  $\mathcal{O}_v$  denote the ring of integers  $\{x \in K_v : |x|_v \leq 1\}$  and  $M_v$  the unique maximal ideal  $\{x \in K_v : |x|_v < 1\}$ . Note that  $\mathcal{O}_v/M_v$  is a finite field; we will write  $q_v$  for its cardinality. We can view the equations defining  $A/K$  as equations over  $K_v$ ; for all but finitely many  $v$ 's, these equations are in  $\mathcal{O}_v$ . We can look at the same equations in  $\mathcal{O}_v/M_v$ .

We say  $v$  is of *good reduction* if we get from  $A$  an abelian variety  $A_v$  over  $\mathcal{O}_v/M_v$ .

**Theorem (Weil).** *Fix  $v \notin S$ . There exists a polynomial  $P_v(T) \in \mathbb{Z}[T]$  such that*

$$P_v(T) = \prod_{i=1}^{2n} (1 - \alpha_i T)$$

where the  $\alpha_i \in \mathbb{C}$  have  $|\alpha_i| = q_v^{\frac{1}{2}}$ , and such that over the finite field  $\mathbb{F}_{q_v^m}$ , for all  $m \geq 1$  we have

$$\#A_v(\mathbb{F}_{q_v^m}) = \prod_{i=1}^{2n} (1 - \alpha_i^m).$$

**Proof.** This is a consequence of Weil's proof of the Riemann Hypothesis for function fields, and is not given here.

**Example.** Elliptic curves  $E/K$  ( $n = 1$ ). Here

$$\#E_v(\mathbb{F}_{q_v}) = (1 - \alpha_1)(1 - \alpha_2) = 1 - (\alpha_1 + \alpha_2) + \alpha_1\alpha_2.$$

Now  $P_v(T) = (1 - \alpha_1 T)(1 - \alpha_2 T) \in \mathbb{Z}[T]$ , because of the above theorem. It follows that if  $\alpha_1 \notin \mathbb{R}$  then  $\alpha_2 = \bar{\alpha}_1$ , and so  $\alpha_1\alpha_2 = |\alpha_1|^2 = q_v$ . If  $\alpha_1 \in \mathbb{R}$ , then  $\alpha_2 \in \mathbb{R}$  and  $\alpha_1, \alpha_2 = \pm q_v^{\frac{1}{2}}$ . If their signs differed, plugging back into  $\#E_v(\mathbb{F}_{q_v})$  would give  $1 - q_v$ , contradicting  $\#E_v(\mathbb{F}_{q_v}) \geq 0$ . We therefore deduce that  $\alpha_1 = \alpha_2$ , and  $\alpha_1\alpha_2 = q_v$ . Hence  $\#E_v(\mathbb{F}_{q_v}) = 1 - (\alpha_1 + \alpha_2) + q_v$ , and we note that  $|\alpha_1 + \alpha_2| \leq |\alpha_1| + |\alpha_2| = 2q_v^{\frac{1}{2}}$ .

We can give an interpretation of  $P_v(T)$  as a characteristic polynomial. Let  $l$  be a prime not dividing  $q_v$ . Then  $A_v[l^k] \subset A_v(\overline{\mathbb{F}_{q_v}})$  is a  $\mathbb{Z}/l^k$ -module of rank  $2n$ . The Frobenius automorphism  $\phi$  (which generates  $Gal(\overline{\mathbb{F}_{q_v}}/\mathbb{F}_{q_v})$ ) acts on  $A_v[l^k]$ .

$P_v(T) = \det(1 - T\phi)$ , so essentially,  $P_v(T)$  is the characteristic polynomial of the Frobenius automorphism.

**Definition.**  $L(A/K, s)$ , a function of the complex variable  $s$ , is given by

$$L(A/K, s) := \prod_{v \notin S} P_v(q_v^{-s})^{-1} \underbrace{\prod_{v \in S} (\text{other stuff})}_{\Psi}$$

where  $\Psi$  is entire and nonvanishing for  $\operatorname{Re}(s) \geq 1$ .

**Exercise.** This product converges for  $\operatorname{Re}(s) > \frac{3}{2}$ .

In the case of elliptic curves over  $\mathbb{Q}$ , we obtain

$$L(E/K, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

where  $1 - a_p + p = \#E_p(\mathbb{F}_p)$ , and  $|a_p| \leq 2p^{\frac{1}{2}}$ . Although  $L$  is strictly only defined for  $\operatorname{Re}(s) > \frac{3}{2}$ , we can heuristically consider  $L(E/\mathbb{Q}, 1)$ . This is

$$\prod_p (1 - a_p p^{-1} + p_{-1})^{-1} = \prod_p \left(\frac{p - a_p + 1}{p}\right)^{-1} = \prod_p \frac{p}{\#E_p(\mathbb{F}_p)}.$$

From the latter expression, if  $\#E_p(\mathbb{F}_p) > p$  “often enough”, then  $L(E/\mathbb{Q}, 1) = 0$ .

We now examine whether the existence of many rational points forces the existence of many points mod  $p$ . Empirically, it has been observed that

$$\prod_{p \leq x} \frac{\#E_p(\mathbb{F}_p)}{p} \longrightarrow \infty \Leftrightarrow E(\mathbb{Q}) \text{ is infinite.}$$

Indeed, if this is the case, then the product grows proportionally to  $(\log x)^r$ , where  $r = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$ .

**Conjecture (Birch, Swinnerton-Dyer).**

(1)  $L(A/K, s)$  has an analytic continuation to  $\mathbb{C}$ .

(2)  $\operatorname{ord}_{s=1} L(A/K, s) = \operatorname{rank}_{\mathbb{Z}} A(K) (= r)$ .

(3)  $\lim_{s \rightarrow 1} (s - 1)^{-r} L(A/K, s) = \frac{R |\text{III}| \prod_{v \in S} c_v}{|A(K)_{\text{tor}}| |A^*(K)_{\text{tor}}|}$ ,

where the regulator  $R = \operatorname{vol}_{\mathbb{R}^r} \left( \frac{A(K)}{A(K)_{\text{tor}}} \right)$  with respect to canonical height,  $\text{III} = \text{III}(A/K)$  is the Tate-Shafarevich group, the  $c_v$  depend on  $\Psi$  above,  $A(K)_{\text{tor}}$  is the subgroup of  $A(K)$  consisting of points of finite order, and  $A^*$  is the dual abelian variety to  $A$ , which we don't define. For elliptic curves,  $A^* = A$ .

**Remarks.** The stronger condition  $(1 \frac{1}{2})$ ,  $L(A/K, 2 - s) = \pm L(A/K, s)$  is known for abelian varieties (over number fields) having “many endomorphisms” by Hecke, Deuring, Taniyama-Shimura and others.

Statement (2) implies that the sign in  $(1 \frac{1}{2})$  is equal to  $(-1)^r$ .

Statements (1) and  $(1\frac{1}{2})$  are known for elliptic curves over  $\mathbb{Q}$  from Wiles' proof of Fermat's Last Theorem.

The statements (1) and  $(1\frac{1}{2})$  are known for abelian varieties over function fields. If  $K/\mathbb{F}_q(t)$ , then  $L(A/K, s)$  is a polynomial in  $q^{-s}$  (Weil, Dwork, Grothendieck). For elliptic curves over  $\mathbb{Q}$ ,  $\text{ord}_{s=1}L(A/\mathbb{Q}, s) \leq 1$  implies statement (2) (Rubin, Kolyvagin, Gross-Zagier, ... )

If  $K$  is a function field, then  $\text{rank}_{\mathbb{Z}}A(K) \leq \text{ord}_{s=1}L(A/K, s)$ , with equality iff  $\text{III}$  is finite. In this case, (2) implies (3) (Tate, ..., Kato-Trihan).