§1. Introduction

A SIMPLE FORMULA CONCERNING MULTIPLICATIVE REDUCTION OF ELLIPTIC CURVES

by Loren D. Olson

The purpose of this note is to show how the coefficients of the canonical invariant differential on an elliptic curve E defined over the field $\mathbf{Q}$ of rational numbers may be used to determine the type of reduction at a prime p where E has bad reduction. Simple and explicit formulas for the coefficients at these primes are obtained. This yields an easy method for calculating the local L-functions at the bad primes. To do this we use a theorem of Honda [2, 3] which says that the formal group F of the curve E is strongly isomorphic over $\mathbf{Z}$ to the formal group G associated to the global L-series of E. We then proceed to analyse the singularity of the reduced curve and obtain the desired formulas. In particular, let E be given by an affine equation $Y^2 = X^3 + AX + B$ with $A, B \in \mathbf{Z}$, which is minimal at a prime $p \geqslant 5$ where E has bad reduction. If $L_p(s) = (1-f_p p^{-s})^{-1}$ is the local L-function at p, then $f_p = \left(\frac{-2AB}{p}\right)$ where $\left(\frac{\ }{p}\right)$ denotes the Legendre symbol at p. Formulas are given for $p = 2$ and $p = 3$ as well.

§1. Introduction

Let K be a field and let E be an elliptic curve defined over K, i.e. a non-singular projective curve of genus one defined over K together with a K-rational point e on E which acts as the identity element for the group law on E. Any such elliptic curve is isomorphic over K to an elliptic curve in the projective plane $\mathbf{P}^2$ defined by the equation

$$(1.1)\quad \overline{Y}^2\overline{Z} + a_1\overline{X}\overline{Y}\overline{Z} + a_3\overline{Y}\overline{Z}^2 = \overline{X}^3 + a_2\overline{X}^2\overline{Z} + a_4\overline{X}\overline{Z}^2 + a_6\overline{Z}^3$$

with $a_i \in K$. The corresponding affine equation is

$$(1.2) \qquad Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

The K-rational point $e = (0, 1, 0)$ is the identity element on this curve. From now on we shall assume that E is given by an equation of this form. Such an equation is called a *Weierstrass equation* for E. Given such an equation, it is usual to define the following invariants:

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1 a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6,$$
$$b_8 = b_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \qquad c_4 = b_2^2 - 24 b_4,$$
$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6,$$

and

$$\Delta = -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6.$$

We note that b_2 and b_4 correspond to Neron's $\bar{\alpha}$ and $\bar{\beta}$ [4, p. 450]. Δ is the *discriminant*. In general if we are given a curve defined by an equation of the form (1.1) or (1.2), it will have a singular point if and only if $\Delta = 0$.

Suppose now that v is a discrete valuation on K normalized so that $v(K^*) = \mathbf{Z}$. Let $R = \{\chi \in K \mid v(\chi) \geqslant 0\}$ be its valuation ring, $M = \{\chi \in K \mid v(\chi) > 0\}$ its maximal ideal, and $k = R/M$ the residue class field. Under the circumstances we may always assume that the coefficients a_i are actually in R. Among all Weierstrass equations with $a_i \in R$, one for which $v(\Delta)$ is minimal is called a *minimal Weierstrass equation* for E. By taking the residue classes of the a_i in k, we obtain from a minimal Weierstrass equation a curve defined over k, the *reduction* of E at v. If the reduction does not have singularities (i.e. $v(\Delta) = 0$), then the reduced curve is an elliptic curve and E is said to have *good reduction*. If the reduction has a singularity (it can have at most one such), then E is said to have *bad reduction*. The singularity may be either a cusp or a node. If the singularity is a cusp, E is said to have *additive reduction*. If the singularity is a node and the two tangents are rational over k, then E has *split multiplicative reduction*. If the singularity is a node and the two tangents are not rational over k, then E has *non-split multiplicative reduction*.

Suppose now that $K = \mathbf{Q}$. Each prime p induces a discrete valuation. Since $\mathbf{Z}$ is a principal ideal domain, it is possible to find a Weierstrass equation which is simultaneously minimal at all primes p, a *global minimal Weierstrass equation*. The primes where E has bad reduction are precisely those which divide Δ. For each prime p we define an integer f_p as follows: $f_p = 0$ if E has additive reduction at p, $f_p = 1$ if E has split multiplicative reduction at p, and $f_p = -1$ if E has non-split multiplicative reduction at p. If E has good reduction at p, let N_p denote the number of $\mathbf{Z}/p\mathbf{Z}$-rational

points of the reduced curve and let $f_p = 1 + p - N_p$. f_p is the trace of Frobenius at p. The *local L-function* $L_p(s)$ *of* E *at* p is defined as $L_p(s) = (1 - f_p p^{-s} + p^{1-2s})^{-1}$ if E has good reduction at p, and $L_p(s) = (1 - f_p p^{-s})^{-1}$ if E has bad reduction at p. The *global L-function* of E is $L(s) = \prod_p L_p(s)$.

If R is a commutative ring, then a (one-dimensional) *formal group* over R is a formal power series $F(X, Y) \in R[[X, Y]]$ in two variables such that $F(X, 0) = X$, $F(0, Y) = Y$, and $F(F(X, Y), Z) = F(X, F(Y, Z))$. Given the global L-function $L(s)$ of an elliptic curve defined over $\mathbf{Q}$, write $L(s) = \sum_{m=1}^{\infty} a_m m^{-s}$. If we set $g(X) = \sum_{m=1}^{\infty} (a_m/m) X^m$ and let $G(X, Y) = g^{-1}(g(X) + g(Y))$, then it can be shown that G is a formal group over $\mathbf{Z}$, the *formal group associated* to $L(s)$. On the other hand, there is another formal group with coefficients in $\mathbf{Z}$ which can be attached to an elliptic curve E defined over $\mathbf{Q}$. If we let $Z = -X/Y$, then Z is a uniformizing parameter in the local ring of E at e. The group law on E is given by a morphism $E \times E \to E$ in which $(e, e) \to e$. We thus have induced a natural homomorphism from the local ring of E at e to $E \times E$ at (e, e). If we complete each of these rings with respect to the topology induced by their respective maximal ideals, we obtain power series rings $\mathbf{Q}[[Z]]$, $\mathbf{Q}[[Z_1, Z_2]]$ in one and two variables over $\mathbf{Q}$. The morphism $E \times E \to E$ induces a local $\mathbf{Q}$-algebra homomorphism $\mathbf{Q}[[Z]] \to \mathbf{Q}[[Z_1, Z_2]]$. The image $F(Z_1, Z_2)$ of Z is then a formal group due to the properties of the group law on E. F has its coefficients in $\mathbf{Z}$. Given two formal groups F and G defined over a commutative ring R, a *homomorphism* $f : F \to G$ *over* R consists of a formal power series $f(T) \in R[[T]]$ such that $f(0) = 0$ and $f(F(X, Y)) = G(f(X), f(Y))$. f is a *strong isomorphism* over R if in addition $f(X) \equiv X \pmod{\text{degree } 2}$ and there exists a homomorphism $g : G \to F$ over R such that $f \circ g = T$ and $g \circ f = T$. A fundamental result which we wish to use here is the following:

THEOREM 1.1 (Honda [2, 3]). Let E be an elliptic curve defined over $\mathbf{Q}$. The formal group F of E is strongly isomorphic over $\mathbf{Z}$ to the formal group G associated to the global L-function of E.

Among all the differentials on E, those which are translation-invariant form a one-dimensional vector space over $\mathbf{Q}$. Given such a differential ω we may expand ω/dZ as a power series in Z. The *canonical invariant differential* on E is the unique one which has 1 as the constant term in this

expansion. Let ω be the canonical invariant differential on E and write $\omega/dZ = \sum_{i=0}^{\infty} C_i Z^i$. It is an immediate consequence of Honda's theorem that $f_p \equiv C_{p-1} \pmod{p}$.

COROLLARY 1.2. Let E be an elliptic curve, and assume that E has bad reduction at a prime p. Then

(1) $C_{p-1} \equiv 0, 1, -1 \pmod{p}$.

(2) E has additive reduction at $p <==> C_{p-1} \equiv 0 \pmod{p}$.

(3) For $p > 2$, E has split multiplicative reduction at $p <==> C_{p-1} \equiv 1 \pmod{p}$.

(4) For $p > 2$, E has non-split multiplicative reduction at $p <==> C_{p-1} \equiv -1 \pmod{p}$.

Proof: Since $C_{p-1} \equiv f_p \pmod{p}$ and $f_p = 0, 1$, or -1, the congruence class of C_{p-1} modulo p determines the reduction type uniquely as indicated except for $p = 2$.

From now on we shall assume that all curves and points are defined over $\mathbf{Q}$, and that all Weierstrass equations are minimal. We wish to derive some simple arithmetical criteria for determining which of the three types of reduction occurs at a given prime p where E has bad reduction. From now on we shall assume that E has bad reduction at the prime p under discussion.

§2. THE CASE $p = 2$

For a curve given in the form (1.2), we have

$$\omega = dX/(2Y + a_1X + a_3) \tag{2.1}$$

Expressing X and Y in terms of Z and computing (cf. Tate [5] for the details), one obtains

$$C_1 = a_1 \tag{2.2}$$

THEOREM 2.1. Assume E has bad reduction at 2.

(1) E has additive reduction at $2 <==> a_1 \equiv 0 \pmod{2} <==> c_4 \equiv 0 \pmod{2}$.

(2) E has split multiplicative reduction at $2 <==> a_1 \equiv 1 \pmod{2}$ and $a_2 + a_3 \equiv 0 \pmod{2}$.