Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 22 (1976)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SIMPLE FORMULA CONCERNING MULTIPLICATIVE REDUCTION OF ELLIPTIC CURVES

Autor: Olson, Loren D.

DOI: https://doi.org/10.5169/seals-48181

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

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

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 $f(X) \equiv X$ (mod 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 $a_2 + a_3 \equiv 0 \pmod{2}$.

(3) E has non-split multiplicative reduction at $2 <=> a_1 \equiv 1 \pmod 2$ and $a_2 + a_3 \equiv 1 \pmod 2$.

Proof: (1). $c_4 \equiv b_2^2 - 24b_4 \equiv b_2^2 \equiv b_2 \equiv a_1^2 + 4a_2 \equiv a_1^2 \equiv a_1 \equiv C_1 \pmod 2$. Now apply Corollary 1.2, part (2).

(2) and (3). By Corollary 1.2, part (2), we have multiplicative reduction $<=> a_1 \equiv 1 \pmod 2$. Assume that this is so. Let $S = (x, y)$ be the singular point. Let

$$H = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \tag{2.3}$$

Compute in $\mathbf{Z}/2\mathbf{Z}$ for the remainder of the proof.

$$\frac{\partial H}{\partial X} = a_1Y - 3X^2 - 2a_2X - a_4 = Y + X^2 + a_4 \tag{2.4}$$

$$\frac{\partial H}{\partial Y} = 2Y + a_1X + a_3 = X + a_3 \tag{2.5}$$

$x = a_3$ from (2.5) and $y = x^2 + a_4 = x + a_4 = a_3 + a_4$ from (2.4). Transform S to $(0, 0)$ via $X \to X + a_3$ and $Y \to Y + a_3 + a_4$. We obtain

$$\begin{aligned} H = {} & (Y+a_3+a_4)^2 + a_1(X+a_3)(Y+a_3+a_4) + a_3(Y+a_3+a_4) \\ & - (X+a_3)^3 - a_2(X+a_3)^2 - a_4(X+a_3) - a_6 \\ = {} & Y^2 + XY + X^3 + (a_2+a_3)X^2 \end{aligned}$$

The tangents at $(0, 0)$ are given by $Y^2 + XY + (a_2+a_3)X^2 = 0$. E has split multiplicative reduction at $2 <=>$ this form is reducible over $\mathbf{Z}/2\mathbf{Z} <=> a_2 + a_3 \equiv 0 \pmod 2$.

§3. The case $p = 3$

As in §2, a short computation (again see Tate [5] for the details) yields

$$C_2 = a_1^2 + a_2 \tag{3.1}$$

THEOREM 3.1. Assume E has bad reduction at 3.

(1) E has additive reduction at $3 \Leftrightarrow a_1^2 + a_2 \equiv 0 \pmod 3$. $\Leftrightarrow c_4 \equiv 0 \pmod 3$.

(2) E has multiplicative reduction at $3 \Leftrightarrow a_1^2 + a_2 \not\equiv 0 \pmod 3 \Leftrightarrow c_4 \not\equiv 0 \pmod 3$.

(3) E has split multiplicative reduction at $3 \Leftrightarrow a_1^2 + a_2 \equiv 1 \pmod 3$.

(4) E has non-split multiplicative reduction at $3 \Leftrightarrow a_1^2 + a_2 \equiv -1 \pmod 3$.

Proof:

$$c_4 \equiv b_2^2 - 24 b_4 \equiv b_2^2 \equiv (a_1^2 + 4a_2)^2 \equiv (a_1^2 + a_2)^2 \pmod 3.$$

The theorem then follows immediately from formula (3.1) and Corollary 1.2.

Remark. $C_2^2 \equiv c_4 \pmod 3$. Note that $C_2 = a_1^2 + a_2$ is a more sensitive invariant than c_4 in that the residue class of C_2 modulo 3 allows us to distinguish between split and non-split multiplicative reduction, while c_4 does not allow us to separate these two possibilities.

§4. The case $p \geqslant 5$

Assume $p \geqslant 5$. Then there exists a minimal Weierstrass equation for E at p of the form

$$Y^2 = X^3 + AX + B \tag{4.1}$$

with A, $B \in \mathbf{Z}$. The coefficient C_{p-1} modulo p is given by Deuring's classical formula [1]

$$C_{p-1} \equiv \sum_{2h+3i=P} \frac{P!}{i!\ h!\ (P-h-i)!} A^h B^i \pmod p \tag{4.2}$$

where $P = (1/2)(p-1)$.

Let $S = (x, y)$ be the singular point on the reduced curve with $x, y \in \mathbf{Z}/p\mathbf{Z}$. The tangents at S are given by a quadratic polynomial $R(T)$ as follows: Transform the curve by $X \to (X+x)$, $Y \to (Y+y)$ so that the singularity is now at (0, 0). The tangents are given by a homogeneous form of degree 2 in X and Y which we can consider as a quadratic polynomial $R(T)$ with $T = Y/X$. Let D be the discriminant of $R(T)$, and let $\left(\frac{\ }{p}\right)$ denote the Legendre symbol with respect to p. We have the following results directly from the definitions.

Proposition 4.1. Assume E has bad reduction at p.

(1) E has additive reduction at $p \Leftrightarrow f_p = 0 \Leftrightarrow S$ is a cusp $\Leftrightarrow R(T)$ has two identical roots over $\mathbf{Z}/p\mathbf{Z} \Leftrightarrow D = 0 \Leftrightarrow \left(\frac{D}{p}\right) = 0$.

(2) E has split multiplicative reduction at $p \Leftrightarrow f_p = 1 \Leftrightarrow S$ is a node with rational tangents $\Leftrightarrow R(T)$ has two distinct roots rational over $\mathbf{Z}/p\mathbf{Z} \Leftrightarrow \left(\frac{D}{p}\right) = 1$.

(3) E has non-split multiplicative reduction at $p \Leftrightarrow f_p = -1 \Leftrightarrow S$ is a node with irrational tangents $\Leftrightarrow R(T)$ has two distinct roots not rational over $\mathbf{Z}/p\mathbf{Z} \Leftrightarrow \left(\frac{D}{p}\right) = -1$.

COROLLARY 4.2. $f_p = \left(\frac{D}{p}\right)$.

In this case, H reduces to

$$H = Y^2 - X^3 - AX - B \tag{4.3}$$

Then we have

$$\partial H / \partial X = -3X^2 - A \tag{4.4}$$

$$\partial H / \partial Y = 2Y \tag{4.5}$$

From (4.5) we must have $y = 0$. From (4.4) we must have $x^2 = -A/3$ in $\mathbf{Z}/p\mathbf{Z}$, so that $-A/3$ is either a quadratic residue modulo p or 0 modulo p. Note that $x = 0 \Leftrightarrow A \equiv 0 \pmod{p}$. Let $X^3 + AX + B = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ be a factorization over $\mathbf{Z}/p\mathbf{Z}$. At least two of $\alpha_1, \alpha_2, \alpha_3$ must coincide with x, let us say $x = \alpha_2 = \alpha_3$. Then

$$X^3 + AX + B = X^3 + (-\alpha_1 - 2\alpha_2) X^2 + (2\alpha_1\alpha_2 + \alpha_2^2) X - \alpha_1\alpha_2^2 \tag{4.6}$$

Thus comparing coefficients, we have

$$0 = -\alpha_1 - 2\alpha_2 \tag{4.7}$$

$$A = 2\alpha_1\alpha_2 + \alpha_2^2 \tag{4.8}$$

$$B = -\alpha_1\alpha_2^2 \tag{4.9}$$

Hence

$$\alpha_1 = -2\alpha_2 \tag{4.10}$$

$$A = 2\alpha_1\alpha_2 + \alpha_2^2 = -3\alpha_2^2 = -3x^2 \tag{4.11}$$

$$B = -\alpha_1\alpha_2^2 = 2\alpha_2^3 = 2x^3 \tag{4.12}$$

From (4.12) we see that $B/2$ is either a cubic residue modulo p or 0 modulo p. Note that $x = 0 \Leftrightarrow B \equiv 0 \pmod{p}$ from (4.12).

Transform the curve by $X \to (X+\alpha_2)$, $Y \to Y$ so that the singular point $S = (x, y) = (x, 0) = (\alpha_2, 0)$ goes to $(0, 0)$. We obtain

$$(4.13) \qquad Y^2 - (X+\alpha_2)^3 - A(X+\alpha_2) - B = Y^2 - X^3 - 3\alpha_2 X^2$$

The tangents to $(0, 0)$ on the transformed curve are given by

$$(4.14) \qquad Y^2 - 3\alpha_2 X^2 = 0$$

so that the polynomial $R(T)$ is $R(T) = T^2 - 3\alpha_2$. $D = 12\alpha_2 = 12x$.

$$c_4 = b_2^2 - 24b_4 = (a_1^2 + 4a_2)^2 - 24(a_1 a_3 + 2a_4) = -48A .$$

Since

$$x = 0 \Leftrightarrow A \equiv 0 \pmod{p}, \quad D = 0 \Leftrightarrow A \equiv 0$$

and so the invariant c_4 is enough to distinguish between additive and multiplicative reduction. However, as we shall see below it does not separate split and non-split multiplicative reduction.

THEOREM 4.3. Assume that E has bad reduction at p.

(1) E has additive reduction at $p \Leftrightarrow A \equiv 0 \pmod{p} \Leftrightarrow B \equiv 0 \pmod{p}$ $\Leftrightarrow \left(\frac{-2AB}{p}\right) = 0.$

(2) E has split multiplicative reduction at $p \Leftrightarrow \left(\frac{-2AB}{p}\right) = 1.$

(3) E has non-split multiplicative reduction at $p \Leftrightarrow \left(\frac{-2AB}{p}\right) = -1.$

Proof: (1) We have seen that $A \equiv 0 \pmod{p} \Leftrightarrow x = 0 \Leftrightarrow B \equiv 0 \pmod{p}$. E has additive reduction at $p \Leftrightarrow D = 12x = 0 \Leftrightarrow x = 0$ $\Leftrightarrow A \equiv B \equiv 0 \pmod{p} \Leftrightarrow \left(\frac{-2AB}{p}\right) = 0.$

(2) and (3). Assume E has multiplicative reduction at p. Then $3\alpha_2 \neq 0$. From (4.14) we see that E has split multiplicative reduction at $p \Leftrightarrow 3\alpha_2$ is a square in $\mathbf{Z}/p\mathbf{Z}$. From formulas (4.11) and (4.12) we have that $3\alpha_2 = (-9/2)\, B/A$. Thus $3\alpha_2$ is a square $\Leftrightarrow (-9/2)\, B/A$ is a square modulo p $\Leftrightarrow -2AB$ is a square modulo $p \Leftrightarrow \left(\frac{-2AB}{p}\right) = 1.$

COROLLARY 4.4. $f_p = \left(\frac{-2AB}{p}\right)$.

§5. Examples

Given an elliptic curve E in the form of a minimal model (1.1) or (1.2), one computes the bad primes by finding the prime divisors of the discriminant Δ. We can then apply the methods of the preceding sections to determine f_p and hence the type of reduction.

Example 5.1. Let E be given by $Y^2 = X^3 + X + 1$. This equation is minimal. The discriminant is $\Delta = -16(31)$, so E has bad reduction at $p = 2$ and $p = 31$. For $p = 2$, $C_{p-1} = C_1 = a_1 = 0$ so we have additive reduction at $p = 2$. For $p = 31$, we can apply Theorem 4.3 and Corollary 4.4. $f_p = \left(\frac{-2AB}{p}\right) = \left(\frac{-2}{31}\right) = -1$, so that E has non-split multiplicative reduction at $p = 31$. Alternatively, one may use Deuring's formula to compute C_{p-1}. A third possibility, of course, is to factor $X^3 + X + 1$ over $\mathbf{Z}/31\mathbf{Z}$ and then analyse (4.14). $c_4 = -48$.

Example 5.2. Let E be given by $Y^2 = X^3 + X - 1$. The equation is minimal and $\Delta = -16(31)$. We have additive reduction at $p = 2$ since $C_{p-1} = C_1 = a_1 = 0$. For $p = 31$, $f_p = \left(\frac{-2AB}{p}\right) = \left(\frac{2}{31}\right) = 1$, so that E has split multiplicative reduction at $p = 31$. $c_4 = -48$.

Remark. Comparing examples 5.1 and 5.2, one sees that c_4 is the same in both cases. However, 5.1. exhibits non-split multiplicative reduction at $p = 31$, while 5.2 exhibits split multiplicative reduction at the same prime.

Example 5.3. Let E be given by $Y^2 = X^3 + 7X + 5$. The equation is minimal and $\Delta = -16(23)(89)$. E has bad reduction at $p = 2, 23$, and 89. For $p = 2$, $C_{p-1} = C_1 = a_1 = 0$, so we have additive reduction at $p = 2$. For $p = 23$, we have $f_p = \left(\frac{-2AB}{p}\right) = \left(\frac{-70}{23}\right) = \left(\frac{-1}{23}\right) = -1$, so that E has non-split multiplicative reduction at $p = 23$. For $p = 89$, we have $f_p = \left(\frac{-2AB}{p}\right) = \left(\frac{19}{89}\right) = -1$, so that E has non-split multiplicative reduction at $p = 89$ as well.

Remark. The computation of the Legendre symbol is much easier to carry out in practice than either the computation of C_{p-1} via Deuring's formula or by searching for roots of the polynomial $X^3 + AX + B$.

BIBLIOGRAPHY

[1] Deuring, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg, 14* (1941), pp. 197-272.

[2] Honda, T. Formal groups and zeta functions. *Osaka J. Math. 5* (1968), pp. 199-213.

[3] —— On the theory of commutative formal groups. *J. Math. Soc. Japan 22* (1970), pp. 213-246.

[4] Neron, A. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *IHES, Publ. Math.* (1964), pp. 361-483.

[5] Tate, J. The arithmetic of elliptic curves. *Inventiones mathematicae, 23* (1974), pp. 179-206.

(Reçu le 5 novembre 1975)

Loren D. Olson

Institute of Mathematical and Physical Sciences
University of Tromsø
P.O. Box 953
N — 9001 Tromsø
Norvège