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.

Kapitel: §4. The case p5

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

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 24.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

(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 $R(T) = T^2 - 3\alpha_2$. $D = 12\alpha_2 = 12x$.

$$c_4 = b_2^2 - 24b_4 = (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4) = -48A\,.$$

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 $p \Leftrightarrow A \equiv 0 \pmod{p} \Leftrightarrow B \equiv 0 \pmod{p}$ $\Leftrightarrow \left(\dfrac{-2AB}{p}\right) = 0.$

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

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

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 $p \Leftrightarrow D = 12x = 0 \Leftrightarrow x = 0$ $\Leftrightarrow A \equiv B \equiv 0 \pmod{p} \Leftrightarrow \left(\dfrac{-2AB}{p}\right) = 0.$

(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 $p \Leftrightarrow \left(\dfrac{-2AB}{p}\right) = 1.$

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