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: §2. The case p= 2

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: 12.01.2026

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

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

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

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 $3 \Leftrightarrow a_1^2 + a_2 \not\equiv 0 \pmod 3 \Leftrightarrow c_4 \not\equiv 0 \pmod 3$.