Zeitschrift: L'Enseignement Mathématique

Band: 22 (1976)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SIMPLE FORMULA CONCERNING MULTIPLICATIVE REDUCTION OF ELLIPTIC CURVES

Kapitel: §3. The case p = 3

Autor: Olson, Loren D.

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

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. 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. Siehe Rechtliche Hinweise.

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. Voir Informations légales.

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. See Legal notice.

Download PDF: 15.10.2024

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

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

(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

(4.1) $$Y^2 = X^3 + AX + B$$

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

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

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 $\mathbf{Z}/p\mathbf{Z} \Leftrightarrow D = 0 \Leftrightarrow \left(\frac{D}{p}\right) = 0$.