

# §5. Examples

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **22 (1976)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

§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  $\Delta$ . 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