A remark on an article of S. Müller

François Morain
INRIA Saclay–Île-de-France
& Laboratoire d'Informatique (CNRS/UMR 7161)
École polytechnique
91128 Palaiseau
France
morain@lix.polytechnique.fr

Version 2 – October 22, 2009

The following proposition proves Conjecture 1 of [2].

Proposition 1 *Let $E : y^2 = F(x) = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_p$ having three rational 2-torsion points. If $p \equiv 3 \bmod 4$, there are no rational 4-torsion points on E.*

Remember Swan's theorem [3]. Let $\left(\frac{a}{p}\right)$ denote the Legendre's symbol.

Theorem 2 *Let $f(X)$ be a squarefree polynomial of degree d and n its number of irreducible factors modulo p. Then*

$$\left(\frac{\mathrm{Disc}(f)}{p}\right) = (-1)^{d-n}.$$

Proof: with the notations of the paper, let the discriminant of E be $\Delta = -16(4a^3 + 27b^2) = 16D$ where $D = \mathrm{Disc}(X^3 + aX + b)$. By hypothesis and Swan's theorem, we get that $(D/p) = +1$. Inspired by [1, §2.2.2], we write $F(X) = (X - e_1)(X - e_2)(X - e_3)$ and get

$$\Delta = 2^4(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 = 16D.$$

The 4-th division polynomial f_4 has three rational quadratic factors

$$\begin{aligned} f_4(X) &= \left(X^2 - 2\,e_1\,X + e_1(e_2 + e_3) - e_2\,e_3\right) \\ &\times \left(X^2 - 2\,e_2\,X + e_2(e_1 + e_3) - e_1\,e_3\right) \\ &\times \left(X^2 - 2\,e_3\,X + e_3(e_1 + e_2) - e_1\,e_2\right) \end{aligned}$$

of respective discriminants $\Delta_1 = 4(e_1 - e_3)(e_1 - e_2)$, $\Delta_2 = 4(e_2 - e_1)(e_2 - e_3)$, $\Delta_3 = 4(e_3 - e_1)(e_3 - e_2)$. Since

$$\Delta_1\Delta_2\Delta_3 = -64D,$$

we deduce that

Fact 1: either one of the Δ_i's is a non-square or all of them are non-squares.

On the other hand, the discriminant of f_4 is $-2^{28}D^5$ so that by Swan's theorem again, we get

$$(\mathrm{Disc}(f_4)/p) = (-D/p) = -1 = (-1)^{6-\omega}$$

and f_4 must have an odd number of irreducible factors, so that

Fact 2: the splitting type of f_4 can be (6), $(4)(1)^2$, (3)(2)(1), $(2)^3$, $(2)(1)^4$.

The only possible way in which we can have both Fact 1 and Fact 2 valid at the same time is that the splitting of f_4 is $(2)^3$, so that f_4 has no rational roots. $\square$

References

[1] F. Morain. Edwards curves and CM curves. `http://hal.inria.fr/inria-00375427/fr`, April 2009.

[2] S. Müller. On the existence and non-existence of elliptic pseudoprimes. *Math. Comp.*, 2009. electronically published October 16, 2009.

[3] R. G. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, 12:1099–1106, 1962.