ACTA ARITHMETICA
142.2 (2010)

Corrigendum to "Distribution of the traces of Frobenius on elliptic curves over function fields"

(Acta Arith. 106 (2003), 255–263)

by

Amílcar Pacheco (Rio de Janeiro)

In Section 4 of [Pa03] we produced three examples of universal elliptic curves over modular curves in which the inequality of Theorem 2.8 was claimed to be an equality (in them the degree of the j-map was replaced by its separable degree). The third example was that of the modular curve $X_1(N)$ and the result was stated in Proposition 4.4.

In fact, this example is invalid: we still have strict inequality there, and the reason is the following. Recall that we are assuming that N is a prime number ℓ different from 2, 3 and p. Let E be an elliptic curve over $\mathbb{F}_{p^k}$ with M rational points and denote by $t := N + 1 - p^k$ its trace of Frobenius. We suppose that $p \nmid t$ and $\ell \mid M$, i.e., $t \equiv p^k + 1 \pmod{\ell}$. If $p^k \not\equiv 1 \pmod{\ell}$, then by [Vo88, Theorem] the ℓ-torsion subgroup of $E(\mathbb{F}_{p^k})$ is cyclic. Therefore, the multiplicity with which E contributes to the sum in [Pa03, (2.2)] is $(\ell-1)/2$ (instead of $(\ell^2-1)/2$ as in Proposition 4.4). If $p^k \equiv 1 \pmod{\ell}$ and $t \equiv p^k + 1 \pmod{\ell^2}$, then the multiplicity with which E contributes to the sum (2.2) is $(\ell^2-1)/2$ if $(\mathrm{Frob}_{p^k} - 1)/\ell \in \mathrm{End}_{\mathbb{F}_{p^k}}(E)$, otherwise it is equal to $(\ell-1)/2$ (cf. [Sc87, Proposition 3.7]), where Frob_{p^k} denotes the Frobenius automorphism of $\mathbb{F}_{p^k}$.

I would like to thank N. Katz for having pointed out this mistake to me in an email. This is the incorrectedness mentioned in the first paragraph of Section 2 of [Ka09].

References

[Ka09] N. M. Katz, *Lang–Trotter revisited*, Bull. Amer. Math. Soc. 46 (2009), 413–457.
[Pa03] A. Pacheco, *Distribution of the traces of Frobenius on elliptic curves over function fields*, Acta Arith. 106 (2003), 255–263.

2010 *Mathematics Subject Classification*: Primary 11G05.

DOI: 10.4064/aa142-2-9

[Sc87] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A 46 (1987), 183–211.

[Vo88] J. F. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France 116 (1988), 455–458.

Amílcar Pacheco
Instituto de Matemática
Universidade Federal do Rio de Janeiro
Rua Guaiaquil 83, Cachambi
20785-050 Rio de Janeiro, RJ, Brasil
E-mail: amilcar.research.math.ufrj.br@gmail.com

Received on 13.7.2009 (6086)