ACTA ARITHMETICA
119.4 (2005)

Erratum: "On the number of prime divisors of the order of elliptic curves modulo p"

(Acta Arith. 117 (2005), 341–352)

by

Jörn Steuding (Madrid) and Annegret Weng (Essen)

There is a serious error in the sieve-theoretical part of the above-mentioned paper: in equation (14), the parameter r has to be chosen as

$$r = [u + 1/\lambda]$$

(as follows from the previous inequality). In the non-CM case, the choice $u = 5.1, v = 20, \lambda = 1.25, \alpha = 1/5.05$ then yields a positive value for $f(u, v, \lambda, \alpha)$, and $r = 6$ instead of $r = 5$; similar changes have to be made for the other cases (when counting distinct prime divisors in the non-CM case resp. the CM case). The main theorem has to be corrected to:

Theorem 1. *Let E be an elliptic curve over $\mathbb{Q}$ such that the finitely many elliptic curves E', $\mathbb{Q}$-isogenous to E, have trivial $\mathbb{Q}$-torsion group. Assume GRH. Then*:

(i) *If E does not have CM*, *then*

$$\sharp\{p \le N : \nu(N_p) \le 6\} \ge C_1 \frac{N}{(\log N)^2},$$

where C_1 is a positive computable constant depending on E; *the inequality for $\nu(N_p)$ can be replaced by $\Omega(N_p) \le 9$.*

(ii) *If E has CM by an order $\mathcal{O}$ in an imaginary quadratic field and χ is the corresponding quadratic character*, *then*

$$\sharp\{p \le N : \chi(p) = 1,\ \Omega(N_p) \le 4\} \ge C_2 \frac{N}{(\log N)^2},$$

where C_2 is a positive computable constant depending on E.

The authors would like to thank Henryk Iwaniec and Jorge Jimenez for pointing out this error.

2000 *Mathematics Subject Classification*: 11N36, 14H42.

Departamento de Matemáticas
Universidad Autónoma de Madrid
C. Universitaria de Cantoblanco
28 049 Madrid, Spain
E-mail: jorn.steuding@uam.es

Institute for Experimental Mathematics
Universität GH Essen
Ellernstr. 29
D-45326 Essen, Germany
E-mail: weng@exp-math.uni-essen.de

Received on 19.8.2005 (5055)