COMPOSITIO MATHEMATICA

Corrigendum

Elliptic curves with a given number of points over finite fields

(Compositio Math. 149 (2013), 175–203)

Chantal David and Ethan Smith

Compositio Math. **150** (2014), 1347–1348.

doi:10.1112/S0010437X14007283

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY

Compositio Math. 150 (2014) 1347–1348
doi:10.1112/S0010437X14007283

Corrigendum

Elliptic curves with a given number of points over finite fields

(Compositio Math. 149 (2013), 175–203)

Chantal David and Ethan Smith

The arithmetic function $K(N)$ defined in the statement of Theorem 3 of [DS13, p. 177] should instead be defined as

$$K(N) := \prod_{\ell \nmid N}\left(1 - \frac{\left(\frac{(N-1)}{\ell}\right)^2 \ell + 1}{(\ell-1)^2(\ell+1)}\right)\prod_{\ell \mid N}\left(1 - \frac{1}{\ell^{\nu_\ell(N)}(\ell-1)}\right).$$

The reasons for the change are a couple of errors in the proof of Lemma 11. In the last line of page 201, the Kronecker symbol $\left(\frac{-N_\ell}{\ell}\right)$ is missing its exponent, and should be replaced by $\left(\frac{-N_\ell}{\ell}\right)^\alpha$. In addition, the sum over $a \in \mathbb{Z}/\ell\mathbb{Z}$ that appears in the line above the last line of page 201 should also carry the condition $4N_\ell + a \neq 0$. The net result is that the statement of Lemma 11 (pp. 188–189) must be altered. In particular, the displayed equation that is the second line of page 189 is not correct. Indeed, in the case that $\ell \mid (N, f)$ and $\nu_\ell(N) = 2\nu_\ell(f)$, we should have

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \#C_N^{(\ell)}(1,1,f)\begin{cases}\left(\ell - 1 - \left(\frac{N_\ell}{\ell}\right)\right) & \text{if } 2 \mid \alpha,\\ -1 & \text{if } 2 \nmid \alpha,\end{cases}$$

instead. This change in the statement of Lemma 11 then affects the computation of the product formula for the arithmetic function $K_0(N) = (N/\varphi(N))K(N)$ that occupies pp. 189–192. The following list outlines the necessary changes.

(1) The function $F_2(\ell, f)$ should instead be defined by

$$F_2(\ell, f) := \begin{cases}\left(1 + \frac{1}{\ell(\ell+1)}\right) & \text{if } \nu_\ell(N) < 2\nu_\ell(f),\\ \left(1 + \frac{1}{\ell}\right) & \text{if } \nu_\ell(N) > 2\nu_\ell(f),\\ \left(1 + \frac{-\left(\frac{N_\ell}{\ell}\right) - 1}{\ell(\ell^2-1)}\right) & \text{if } \nu_\ell(N) = 2\nu_\ell(f).\end{cases}$$

Received 3 December 2013, accepted in final form 6 February 2014, published online 17 July 2014.
2010 Mathematics Subject Classification 11G05 (primary), 11N13 (secondary).
Keywords: average order, elliptic curves, primes in short intervals, Barban–Davenport–Halberstam theorem, Cohen–Lenstra heuristics.

(2) If $\nu_\ell(N) > 0$, then in all cases (that is, whether $\nu_\ell(N)$ is odd or even and whether $\left(\frac{N_\ell}{\ell}\right) = \pm 1$), we find that

$$1 + \sum_{\alpha \geqslant 1} \frac{\# C_N^{(\ell)}(1, 1, \ell^\alpha) F_2(\ell, \ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha} F_0(\ell)} = 1 + \frac{\ell^{\nu_\ell(N)} - \ell}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell - 1)^2}.$$

(3) Eventually, we arrive at the following corrected product formula for $K_0(N)$:

$$K_0(N) = \frac{N}{\varphi(N)} \prod_{\ell \nmid N} \left(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \ell + 1}{(\ell - 1)(\ell^2 - 1)}\right) \prod_{\ell \mid N} \left(1 - \frac{1}{\ell^{\nu_\ell(N)}(\ell - 1)}\right).$$

Reference

DS13 C. David and E. Smith, *Elliptic curves with a given number of points over finite fields*, Compositio Math. **149** (2013), 175–203.

Chantal David cdavid@mathstat.concordia.ca
Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montréal, Québec, H3G 1M8, Canada

Ethan Smith ecsmith13@liberty.edu
Department of Mathematics, Liberty University, 1971 University Boulevard, MSC Box 710052, Lynchburg, VA 24502, USA

https://doi.org/10.1112/S0010437X14007283 Published online by Cambridge University Press