Let $\omega(n)$ denote the number of distinct prime factors of $n \in \mathbb{N}$, and let $E/\mathbb{Q}$ be an elliptic curve of rank $\geq 1$, with $b \in E(\mathbb{Q})$ being a rational point of finite order. For a prime $p^*$ of good reduction denote by $(\overline{b})$ the cyclic group generated by the reduction $\overline{b}$ of $b$ modulo $p^*$, and let $g_b(p^*)$ be its order. Assuming a certain Generalized Riemann Hypothesis (GRH), the two results proved in this paper are the following:

For all $x \geq 0$,

$$\sum_{p^* \leq x} (\omega(g_b(p^*)) - \log \log(p^*))^2 \ll \pi(x) \log \log x,$$

and, for any $\gamma \in \mathbb{R}$, as $x \to \infty$

$$\frac{\sqrt{2\pi}}{\pi(x)} \# \left\{ p^* \leq x: \frac{\omega(g_b(p^*)) - \log \log(p^*)}{\sqrt{\log \log(p^*)}} \leq \gamma \right\} \sim \int_{-\infty}^{\gamma} e^{-t^2/2} \, dt,$$

i.e., the distribution of the quantity in question is normal.


Reviewed by Filip Saidak
[References]

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.


16. S. A. Miri and V. K. Murty, An application of sieve methods to elliptic curves. In Progress in

© Copyright American Mathematical Society 2006