

ON THE AVERAGE EXPONENT OF ELLIPTIC CURVES MODULO p

TRISTAN FREIBERG

ABSTRACT. Given an elliptic curve E defined over \mathbb{Q} and a prime p of good reduction, let $\tilde{E}(\mathbb{F}_p)$ denote the group of \mathbb{F}_p -points of the reduction of E modulo p , and let e_p denote the exponent of this group. Assuming a certain form of the Generalized Riemann Hypothesis, we study the average of e_p as $p \leq X$ ranges over primes of good reduction, and find that the average exponent essentially equals $p \cdot c_E$, where the constant $c_E \in (0, 1)$ depends on E .

This is joint work with Pär Kurlberg.