

ELLIPTIC CURVES, SIEVES AND CRYPTOGRAPHY

(Joint work with C. David)

ABSTRACT. In this talk, I shall present my recent joint works with Chantal David. Let E be an elliptic curve over \mathbb{Q} without complex multiplication. For each prime p of good reduction, let $|E(\mathbb{F}_p)|$ be the order of the group of points of the reduced curve over \mathbb{F}_p . According to a conjecture of Koblitz, there should be infinitely many such primes p such that $|E(\mathbb{F}_p)|$ is prime, unless there are some local obstructions predicted by the conjecture. Suppose that E is a curve without local obstructions (which is the case for most elliptic curves over \mathbb{Q}). Firstly we prove that, under the GRH, there are at least $2.778C_E^{\text{twin}}x/(\log x)^2$ primes p such that $|E(\mathbb{F}_p)|$ has at most 8 prime factors, counted with multiplicity. This improves previous results of Steuding & Weng and Miri & Murty. This is also the first result where the dependence on the conjectural constant C_E^{twin} appearing in Koblitz's conjecture (also called the twin prime conjecture for elliptic curves) is made explicit. Secondly we can also improve the constant of Zywinina appearing in the upper bound for the number of primes p such that $|E(\mathbb{F}_p)|$ is prime. Finally motivated by cryptography applications, we study elliptic pseudoprimes to the base b . Let $Q_{E,b}(x)$ be the number of primes $p \leq x$ such that $b^{n_E(p)} \equiv b \pmod{n_E(p)}$, and $\pi_{E,b}^{\text{pseu}}(x)$ be the number of *compositive* $n_E(p)$ such that $b^{n_E(p)} \equiv b \pmod{n_E(p)}$ (also called elliptic curve pseudoprimes). We address the problem of finding upper bounds for $Q_{E,b}(x)$ and $\pi_{E,b}^{\text{pseu}}(x)$, generalising some of the literature for the classical pseudoprimes of Erdős and Pomerance to this new setting.