**CHANTAL DAVID**, Concordia University

*Almost prime orders of elliptic curves over finite fields*

Let $E$ be an elliptic curve over the rationals. A conjecture of Neal Koblitz predicts an exact asymptotic for the number of primes $p$ such that the order of $E$ over the finite field with $p$ element is prime. This conjecture is still open. Using sieve techniques, one can find a lot of primes $p$ such that the order $p+1-a_P(E)$ is almost prime. The best result that one may hope to achieve by sieve techniques was obtained by Iwaniec and Jimenez Urroz for complex multiplication curves using Chen's sieve. They showed that there are infinitely many primes $p$ such that $p+1-a_p(E) = P_2$, where $n = P_k$ means that the integer $n$ has at most $k$ prime factors. For elliptic curves without complex multiplication, it is not known how to apply the switching principle of Chen's sieve to get such a result.

For curves without complex multiplication, we show that there are many primes $p$ such that $p+1-a_p(E) = P_8$ with an explicit lower bound (in terms of the constant $C(E)$ of Koblitz's conjecture), using Greaves' sieve and under the GRH. This improves previous work of Steuding and Weng. One can also show that there are many primes such that $p+1-a_p(E)$ has at most 6 *distinct* prime factors, but still cannot improve the number of (not necessarily distinct) primes from 8 to 6. This surprising result is related to the difficulty of sieving square-free numbers in the sequence $p+1-a_p(E)$.

This is joint work with Jie Wu (CNRS, Institut Elie-Cartan, Nancy).