

---

**DIMITRIS KOUKOULOPOULOS**, Université de Montréal

*Groups structures of elliptic curves over finite fields*

It is known that an elliptic curve  $E$  over a finite field  $\mathbb{F}_p$  admits a group structure which is abelian and has rank at most 2. Therefore there are integers  $m$  and  $k$  such that the group of points of  $E$  over  $\mathbb{F}_p$  is isomorphic to  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ . In the converse direction, Rück characterized which pairs of integers  $(m, k)$  can arise this way. It is then natural to ask how many of such pairs exist with  $m \leq M$  and  $k \leq K$ . Call the number of such pairs  $S(M, K)$ . Banks, Pappalardi and Shparlinski studied the size of  $S(M, K)$ , which they related to a problem about the existence of primes in short arithmetic progressions. Based on standard heuristics about primes, they made a conjecture about the size of  $S(M, K)$  and proved some partial results towards it. In this talk, I will discuss recent progress in this problem which leads to an improvement of the results of Banks, Pappalardi and Shparlinski, as well as to a proof of their conjecture in certain ranges of  $M$  and  $K$ . This is joint work with V. Chandee, C. David and E. Smith.