Atelier
« Nouvelles approches en théorie probabiliste et multiplicative des nombres »
08-12 décembre 2014

Workshop
"New approaches in probabilistic and multiplicative number theory"
December 08–12, 2014

Statistics associated with reductions of elliptic curves modulo p

Paul Pollack [*]

pollack@math.uga.edu

Fix an elliptic curve $E/\mathbf{Q}$. For each prime p of good reduction, one can reduce E to obtain an elliptic curve defined over the finite field $\mathbf{F}_p$. It is natural to investigate how the structure of the groups $E(\mathbf{F}_p)$ varies with p. The prototypical result is due to Serre: Suppose E has an irrational 2-torsion point. Then, assuming GRH, the group $E(\mathbf{F}_p)$ is cyclic for a well-defined positive proportion of primes p. If E has complex multiplication (CM), then the GRH assumption can be dropped, as shown first by Ram Murty and later in a simpler way by Cojocaru.

After reviewing some other results in this direction, we discuss two recent projects of the speaker (the second joint with T. Freiberg). The first concerns the average value of $\tau(\#E(\mathbf{F}_p))$ over primes $p \le x$, where τ is the divisor function. This is an elliptic curve analogue of the Titchmarsh divisor problem. To explain the second topic, recall that $E(\mathbf{F}_p)$ is a finite abelian group of rank two and so can be written as $\mathbf{Z}/d_p\mathbf{Z} \oplus \mathbf{Z}/e_p\mathbf{Z}$, where $d_p \mid e_p$. (Thus, e_p is the exponent of the group.) Freiberg and Kurlberg have given an asymptotic formula for the average value of e_p (unconditionally in the CM case and conditional on GRH in the non-CM case). We discuss recent progress estimating the average value of d_p, in the case when E has complex multiplication.

[*]Department of Mathematics, University of Georgia, Boyd Graduate Research Center, Athens, GA 30602, USA.