AMIR AKBARY, University of Lethbridge

On the moments of torsion points modulo primes

Let $\mathbb{A}[n]$ be the group of n-torsion points of a commutative algebraic group $\mathbb{A}$ defined over a number field F. For a prime ideal $\mathfrak{p}$ of F that is unramified in $F(\mathbb{A}[n])/F$, we let $N_{\mathfrak{p}}(\mathbb{A}[n])$ be the number of $\mathbb{F}_{\mathfrak{p}}$-solutions of the system of polynomial equations defining $\mathbb{A}[n]$ when reduced modulo $\mathfrak{p}$. Here, $\mathbb{F}_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. Let $\pi_F(x)$ denote the number of prime ideals $\mathfrak{p}$ of F whose norm $N(\mathfrak{p})$ do not exceed x. We then, for algebraic groups of dimension one, compute the k-th moment limit

$$M_k(\mathbb{A}/F,n) = \lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\leq x} N_{\mathfrak{p}}^k(\mathbb{A}[n])$$

by appealing to the prime number theorem for arithmetic progressions and more generally the Chebotarev density theorem. We further interpret this limit as the number of orbits of $\mathrm{Gal}(F(\mathbb{A}[n])/F)$ acting on k copies of $\mathbb{A}[n]$ by another application of the Chebotarev density theorem. These concrete examples suggest a possible approach for determining the number of orbits of a group acting on k copies of a set.

This is a joint work with Peng-Jie Wong (University of Lethbridge).