New Directions in Combinatorics (9 - 27 May 2016)

Dirk Hachenberger
Institut für Mathematik der Universität Augsburg, 86135 Augsburg, Germany
hachenberger@math.uni-augsburg.de

Title of talk:

Ovoids and primitive normal bases for quartic extensions of Galois fields

Abstract:

By a celebrated result of H. W. Lenstra, Jr. and R. J. Schoof (1987), any extension E/F of Galois fields admits a generator of the multiplicative group of E whose conjugates under the Galois group are linearly independent over F. Any such element is called a *primitive normal basis generator* for E/F. We present a lower bound for the number of such elements in the case where $E = \mathrm{GF}(q^4)$ is the quartic extension over $F = \mathrm{GF}(q)$.

Our approach is geometric: Considering E as the three-dimensional projective space $\Gamma = \mathrm{PG}(3, q)$, the points of that space are distinguished into primitive and non-primitive ones. The structure of the multiplicative group of E gives rise to a partition of the point set of Γ into $q + 1$ ovoids. The bound is derived by studying the intersection of those ovoids which cover the primitive points with the non-normal configuration; the latter is the collection of points of Γ which do *not* give rise to normal elements of E/F.

Given that $q^2 + 1$ is a prime number when q is even, or that $\frac{1}{2}(q^2 + 1)$ is a prime number when q is odd, we actually achieve the exact number of all primitive normal elements for the quartic extension over $\mathrm{GF}(q)$. Moreover, the proportion of all primitive normal elements among all primitive elements converges to 1 as q tends to infinity. For instance, when $q \geq 79$, then at least 95 percent of all primitive elements of $\mathrm{GF}(q^4)$ are normal over $\mathrm{GF}(q)$.