UF Algebra Seminar

Eric Moorhouse, University of Wyoming

Title: Ovoids from Lattices

Abstract:

Theorem I. Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}_p$ be the set of all 6-tuples $(x_1, \ldots, x_6)$ of integers $x_i \equiv 1 \bmod 4$ such that $x_1^2 + \cdots + x_6^2 = 6p$. Then $|\mathcal{S}_p| = p^3 + 1$.

Check this for $p = 5, 13$! You may be aware of some general techniques (possibly using modular forms) which suffice to prove results of this nature. But elementary considerations from geometry offer an easier proof with deeper insight into the nature of the set $\mathcal{S}_p$. Namely, $\mathcal{S}_p$ determines a set of $p^2 + 1$ points of projective 5-space over $\mathbb{F}_p$ with a special property: These points all lie on a nondegenerate quadric $\mathcal{Q}$. The quadric contains $(p^2 + p + 1)(p^2 + 1)$ planes; and each of these planes contains a unique point of $\mathcal{S}_p$. Such a point set is called an *ovoid* of the quadric $\mathcal{Q}$.

The E_8 *root lattice* is the unique lattice $E \subset \mathbb{R}^8$ (i.e. $\mathbb{Z}$-submodule of rank 8) which is integral, even and unimodular (i.e. $\mathbf{u} \cdot \mathbf{v} \in \mathbb{Z}$, $\mathbf{v} \cdot \mathbf{v} \in 2\mathbb{Z}$ for all $\mathbf{u}, \mathbf{v} \in E$; also $\{\mathbf{u} \in \mathbb{R}^8 : \mathbf{u} \cdot \mathbf{v} \in \mathbb{Z} \text{ for all } \mathbf{v} \in E\} = E$; and 'unique' means up to isometry). Fix $\mathbf{e} \in E$ satisfying $\mathbf{e} \cdot \mathbf{e} = 2$. (There are 240 such vectors, the *roots* of the lattice.) Consider the sublattice $L = \mathbb{Z}\mathbf{e} + 2E \subset E$.

Theorem II. Given an odd prime p, let $\mathcal{O}_p$ be the set of all $\mathbf{v} \in L$ such that $\mathbf{v} \cdot \mathbf{v} = 2p$. Then $\mathcal{O}_p$ consists of $p^3 + 1$ pairs $\pm\mathbf{v}$; and these points form an ovoid in a nondegenerate quadric of projective 7-space over $\mathbb{F}_p$.

The ovoids of Theorem II were constructed by Conway, Kleidman and Wilson (1988) and generalized by the speaker (1993). 'Slices' of these ovoids give hosts of ovoids in smaller dimensions, including those of Theorem I.