REGINALD SIMPSON, University of British Columbia

The Density and Distribution of Cyclic Groups in the Invariant Factor Decomposition of the Multiplicative Group

For any integer m the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^{\times}$ has a unique decomposition into a product of cyclic groups $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_N}$ where $d_i \mid d_{i+1}$ for $1 \leq i < N$, called the invariant factor decomposition. In this talk we discuss three results from a forthcoming paper concerning this decomposition, and the techniques used to prove those results. First, for any order d: we determine the natural density of m where $\mathbb{Z}_d$ is in the invariant factor decomposition of m. Second, for any order d: we determine asymptotic formulas (in terms of some n) for how many copies of $\mathbb{Z}_d$ are there on average in the invariant factor decomposition of m in the range $1 \leq m \leq n$. Third, for any order d: we determine Erdős-Kac-like limiting distributions for the number of copies of $\mathbb{Z}_d$ in the invariant factor decomposition of the multiplicative group. The details of these results reveal a delightfully elegant pattern and the discussion of the proof techniques will demonstrate why this pattern is, when thought about carefully, intuitive.