Speaker: Zachary Scherr

Title: Capacity Theory and Optimality of Coppersmith's Theorem

Abstract: Coppersmith's method is an approach to finding small integral solutions to polynomial congruences. Given a monic polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree $d > 1$ and a positive integer N, Coppersmith devised a polynomial time method for finding all rational integers r for which $f(r) \equiv 0 \pmod{N}$ and $|r| < N^{1/d}$. In this talk we will show a connection between Coppersmith's method and adelic capacity theory, as developed by Cantor and Rumely. We will be able to use results from capacity theory to prove that the $N^{1/d}$ is sharp in Coppersmith's method. We will also explain why proposed refinements to Coppersmith's method cannot succeed unless N has a *"small"* prime factor.

This is joint work with Ted Chinburg, Brett Hemenway and Nadia Heninger.