1125-11-841 **Ted Chinburg**, **Brett Hemenway**, **Nadia Heninger** and **Zachary Scherr*** (zls002@bucknell.edu). *Capacity Theory and Optimality of Coppersmith's Theorem.*

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 integers r for which

$$f(r) \equiv 0 \mod N$$

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. Time permitting, we will also show why proposed modifications to Coppersmith's algorithm still cannot break this barrier for N of cryptographic interest. This is joint work with Ted Chinburg, Brett Hemenway and Nadia Heninger. (Received September 12, 2016)