SARAH PELUSE, Institute for Advanced Study

An asymptotic version of the prime power conjecture for perfect difference sets

A set $D \subset \mathbb{Z}/m\mathbb{Z}$ is called a "perfect difference set" if every nonzero element of $\mathbb{Z}/m\mathbb{Z}$ can be written uniquely as the difference of two elements of D. If such a set exists, then $m = n^2 + n + 1$ for some nonnegative integer n. Singer constructed perfect difference sets in $\mathbb{Z}/(n^2 + n + 1)\mathbb{Z}$ whenever n is a prime power, and it is an old conjecture that these are the only such n for which a perfect difference set exists. I will discuss a proof of an asymptotic version of this conjecture: the number of $n \leq N$ for which $\mathbb{Z}/(n^2 + n + 1)\mathbb{Z}$ contains a perfect difference set is $\sim \frac{N}{\log N}$.