CHI HOI (KYLE) YIP, University of British Columbia

Additive decompositions of multiplicative subgroups

A celebrated conjecture of Sárközy asserts that if p is a sufficiently large prime, then the set of non-zero squares in $\mathbb{F}_p$ has no non-trivial additive decomposition, that is, it cannot be written as $A+B=\{a+b : a\in A, b\in B\}$, where $A,B\subset\mathbb{F}_p$ and $|A|,|B|\geq 2$. The conjecture is widely open. In this talk, I will focus on the restricted sumset analog of Sárközy's conjecture. More precisely, we show that if $q>13$ is an odd prime power, then the set of nonzero squares in $\mathbb{F}_q$ cannot be written as a restricted sumset $A\hat{+}A$. More generally, I will discuss related results for multiplicative subgroups over finite fields.