DANIEL KATZ, California State University, Northridge
Valuations of Weil Sums of Binomials

Weil sums of binomials are finite field character sums that arise naturally in number theory and its technological applications. In cryptography, such sums determine the Walsh spectrum of a power permutation of a finite field, which measures its nonlinearity. Weil sums of binomials also determine the cross-correlation between two maximal linear sequences in digital sequence design and the weight distribution of certain cyclic error-correcting codes. Consider the Weil sum

$$W_{q,d}(a) = \sum_{x \in \mathbf{F}_q} \psi_q(x^d - ax),$$

where

- ψ_q is the canonical additive character of finite field $\mathbf{F}_q$,
- $\gcd(d, q-1) = 1$, so that $x \mapsto x^d$ is a permutation of $\mathbf{F}_q$,
- d is not a power of p modulo $q-1$, to prevent $\psi_q(x^d - ax)$ degenerating to $\psi_q((1-a)x)$, and
- $a \in \mathbf{F}_q$.

Let v_p be the p-adic valuation, and for fixed q and d let

$$V_{q,d} = \min_{a \in \mathbf{F}_q} v_p(W_{q,d}(a)),$$

so that $V_{q,d}$ indicates the p-divisibility of the entire Walsh spectrum $\{W_{q,d}(a) : a \in \mathbf{F}_q\}$. We present a proof that $V_{q,d}$ is never more than $2n/3$, where $q = p^n$. We also present stronger upper bounds in special cases and discuss some conjectures. This is joint work with Philippe Langevin of Université de Toulon and Sangman Lee and Yakov Sapozhnikov of California State University, Northridge.