Equidistribution of Roots of a Quadratic Congruence

Speaker: Matthew Welsh

Consider the set of fractions $\frac{\nu}{m} \in \mathbb{R}/\mathbb{Z}$ such that $\nu^2 \equiv -1 \pmod{m}$, ordered by the modulus m (the ordering of the roots with the same modulus is immaterial). Hooley proved in 1963 that this sequence is equidistributed (mod 1), a fact that is equivalent, by Weyl's criterion, to showing $\sum_{m \leq M} e(\frac{\nu}{m}) = o(M)$. Getting bound on this (and similar sums) formed a crucial step in Iwaniec's 1978 proof that there are infinitely many n^2+1 that are the product of ≤ 2 primes.

In 1983, Bykovsky produced the (optimal) bound $O(M^{1/2+\epsilon})$ for (a smoothed version of) the above Weyl sum by relating it to a Poincaré series on $SL_2(\mathbb{Z})\backslash\mathbb{H}$ in what I see as one of the most spectacular applications of the spectral theory of automorphic forms (probably the most spectacular to me is Duke, Friedlander, and Iwaniec's proof that the sequence is still equidistributed after restricting m to be a prime). After elaborating a bit on what has been said here, in this talk I will explain this Bykovsky's relation via the theory of binary quadratic forms (or, depending on audience interest, ideals in quadratic number fields), and indicate how spectral theory would help in estimating the resulting Poincaré series (either by bounds for fourier coefficients of automorphic forms via a spectral expansion, or by transforming directly to sums of Kloosterman sums).