Speaker: Kristin Lauter

Title: On a Generalization of Gross-Zagier and applications to Genus 2 Curves in Cryptography

Abstract: The modular j-function plays an important role in number theory: its values at quadratic imaginary integers are called singular moduli. Singular moduli can be interpreted as an invariant of CM elliptic curves and play a role in explicit class field theory. In 1985, Gross and Zagier gave an elegant formula for the factorization of norms of differences of singular moduli associated to a pair of imaginary quadratic discriminants d_1 and d_2, under the assumption that d_1 and d_2 are fundamental and relatively prime. Their theorem was one of the ingredients in the proof of the only known case of the Birch-Swinnerton Dyer Conjecture. This talk will present a generalization of their result to give a complete factorization for any two fundamental discriminants which are not necessarily coprime, and obtain at least a partial factorization for any two quadratic imaginary discriminants. We will discuss the motivation for this generalization arising in cryptography and give an application to proving an intersection formula on Hilbert modular surfaces related to the work of Bruinier and Yang. The proof relies on a characterization of solutions to the embedding problem posed by Goren and Lauter which involves counting the same quantities which are counted in the Gross-Zagier formula. This is joint work with Bianca Viray.

RTG Abstract: Applications to Cryptography: can genus 2 curves beat genus 1 curves in performance vs. security?