"Curves, Cryptography and Calculus: A Weil pairing on Elliptic Curves over the Dual Numbers"

Monday, December 3, 2007

Talk at 4:15 - Park 338
Tea at 3:45 - Park 355, Math Lounge

Abstract:

First proposed in 1985, elliptic curve cryptosystems are now widely used by government and industry and represent an active area of research for mathematicians. I will introduce elliptic curves and the basic idea of elliptic curve cryptography, and show how the Weil pairing on the points of order $n$ of an elliptic curve over a field $K$ with characteristic prime to $n$ is used to attack the security of certain cryptosystems.

I will then discuss my work with elliptic curves over the dual numbers of $K$, the set of elements of the form $a + be$ where $a, b$ are in $K$ and $e^2 = 0$. These numbers behave like numbers with extra "derivative" information-their arithmetic mimics the basic rules of calculus. I will show how in working over the dual numbers, we can extend the Weil pairing to points of order $p$ where $p$ is relatively prime to the characteristic of $K$. In doing so, we recover an attack on trace one elliptic curves, which was first discovered in 1999.