Number Theory Seminar

Organizer: Bjorn Poonen

Wednesday, 3:10–4:00pm, 334 Evans

Oct. 18 **Michael D. Fried**, UC Irvine (Emeritus), MSU-Billlings
The Exceptional Tower of a variety over a finite field

Let Y be a normal (absolutely irreducible) variety over a finite field $\mathbb{F}_q$. An exceptional cover $X \to Y$ over $\mathbb{F}_q$ is a cover of normal varieties with the map on $\mathbb{F}_{q^t}$-points one-one for infinitely many t. Exceptional covers of $(Y, \mathbb{F}_q)$ form a category with fiber products. So there is a well-defined exceptional tower. I will outline its construction, and describe in some subtowers. The most well-known subtower for $(\mathbb{P}^1, \mathbb{F}_q)$ is given by the collection of maps $\mathbb{P}^1_x \to \mathbb{P}^1_z$ by $x \mapsto x^n$, with $(n, q-1) = 1$. The exceptional tower of any $(Y, \mathbb{F}_q)$ is a natural place for cryptography. There are also versions over number fields, and both have their applications. I'll say something about the following two. Cryptography questions in the number field case naturally extend questions on Serre's Open Image Theorem (action of an absolute Galois group on elliptic curve division points; especially his Tchebotareff Density paper). Exceptional covers generalize to strong Davenport pairs. These give universal relations among Poincaré series defined by diophantine problems over finite fields. For understanding Chow motives we would like to know if all relations come from strong Davenport pairs. Example: If the Poincaré series of a curve over $\mathbb{F}_q$ has its t-th coefficient equal to $q^t + 1$ for infinitely many t, is there a chain of exceptional correspondences from the curve to $\mathbb{P}^1$?