Special Stanford Number Theory / Algebraic Geometry Seminar

REVISITING THE p-ADIC APPROACH TO ZETA FUNCTIONS: FROM THEORY TO ALGORITHMS

KIRAN KEDLAYA
M.I.T.

Abstract

To an algebraic variety over a finite field, there is a natural way to associate a zeta function, a suitable generating function counting rational points on the variety over all of the finite extensions of the ground field. Weil conjectured that this function, which is defined as a power series in one variable, always represents a rational function. Nowadays this, the first of the celebrated Weil conjectures, is typically proved by invoking properties of etale cohomology, as developed by Grothendieck et al; the technique proves strong theorems but is not particularly amenable to computations. (They also don't shed much light on the nature of "arithmetic" zeta functions, e.g., those associated to number fields.) However, the first proof of rationality was given by Dwork, using a completely different approach rooted in p-adic analysis. Later several authors (Monsky-Washnitzer, Grothendieck, Berthelot) realized that Dwork's methods also admit a "cohomological" interpretation, although work on establishing a fully functional theory is ongoing. (For instance, it is only recently that the theory has progressed far enough to be able to simulate Deligne's etale-cohomological proof of Weil's analogue of the Riemann Hypothesis.) Even later, it was realized that Dworkian methods are relevant in computational number theory (in applications where varieties over finite fields occur, e.g., coding theory, cryptography); I'll describe enough of the theory to illustrate an explicit example of this, a good algorithm for computing zeta functions of hyperelliptic curves. I may engage in some mild speculation on what other algorithms remain to be described. (I may also engage in some wild speculation on what any of this has to do with arithmetic zeta functions.)

Thursday, May 19
noon
Room: 383-N

http://math.stanford.edu/~vakil/s0405/