Arizona Winter School 2007
p-adic cohomology: from theory to practice
Kiran Kedlaya

Course description

The goal of this course is to illustrate how p-adic analytic methods can be used to construct explicit Weil cohomology for varieties over finite fields. The sense in which "explicit" is meant here is that if one starts with a variety defined by specific equations, one can in principle compute good approximations to the matrix via which Frobenius acts on some basis of cohomology. (Since this matrix has p-adic coefficients, one cannot expect to compute it exactly, any more than one can exactly compute a typical real number.)

We will start with the Monsky-Washnitzer cohomology of a smooth affine variety over a finite field. This includes constructing the cohomology using a lift to characteristic zero, checking independence of the construction from choices, proving an excision formula, and checking the Lefschetz trace formula. (This all follows the original papers of Monsky-Washnitzer.) By sheafifying, we will obtain a cohomology theory for general smooth varieties, which is Berthelot's rigid cohomology (also known as crystalline cohomology with field coefficients).

We will then formulate the comparison theorem between rigid cohomology and de Rham cohomology for a smooth proper scheme over $\mathfrak{o}_K$, the ring of integers in a p-adic field K. This means that the de Rham cohomology of a variety over K with good reduction carries a Frobenius action, even though the Frobenius map on the special fibre does not typically lift to characteristic zero. It also means that we can use what we know about the de Rham cohomology of the generic fibre to compute the zeta function of the special fibre; this paradigm, applied to hyperelliptic curves as in [3], forms the basis of applications of p-adic cohomology in cryptography (the "practice" of the title).

We will then consider Gauss-Manin connections from the algebraic point of view (following [2]), with an eye towards using these to compute Frobenius actions in de Rham cohomology (following Lauder). This theme will be carried further in the project.

Project description

The project will involve computing examples of Frobenius actions on the de Rham cohomology of smooth proper varieties over a finite extension K of $\mathbb{Q}_p$ which have semistable, rather than good, reduction. (Everywhere in this description, "compute" means "compute on a computer", using *SAGE*.) The existence of such Frobenius actions is due to Hyodo and Kato; however, unlike in the good reduction situation, it is not completely canonical. This failure of canonicity is explained by the nonvanishing of a second operator, the monodromy operator, which is indeed zero in the good reduction case.

We will first compute the Hyodo-Kato Frobenius and monodromy actions on elliptic curves using the Tate uniformation (following [4, 1]). We will then recompute it (at least conjecturally; if time permits, we may try to prove correctness of these results using [1]) using Gauss-Manin connections, particularly in the Legendre family (the universal family of elliptic curves with rational 2-torsion). One key question we will be investigating, to which I don't know the answer: if one encounters an elliptic curve with multiplicative reduction in a family such as the Legendre family, one apparently gets some Hyodo-Kato Frobenius on its de Rham cohomology from the global Frobenius action on the connection, but which one?

References

[1] R. Coleman and A. Iovita, The Frobenius and monodromy operators for curves and abelian varieties. *Duke Math. J.* 97 (1999), no. 1, 171–215.

[2] N.M. Katz and T. Oda, On the differentiation of de Rham cohomology classes with respect to parameters. *J. Math. Kyoto Univ.* **8** (1968), 199–213.

[3] K.S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), 323–338; errata, *ibid.* **18** (2003), 417–418.

[4] B. le Stum, La structure de Hyodo-Kato pour les courbes, *Rend. Sem. Mat. Univ. Padova* **94** (1995), 279–301.