ARITHMETIC OF ELLIPTIC CURVES OVER FUNCTION FIELDS (NUMBER THEORY SEMINAR, BERKELEY, SPRING 2015)

XINYI YUAN

The BSD conjecture, usually stated for elliptic curves over number fields, can be similarly formulated for abelian varieties over global fields. In fact, when restricted to global function fields, much more is known about the conjecture. The most striking known result is that the BSD conjecture for (all) abelian varieties over global function fields is equivalent to the Tate conjecture for (all) surfaces over finite fields. For quick overview of the theory, we refer to Douglas Ulmer's surveys [Ul1, Ul2].

The goal of this seminar is to study the BSD conjecture over global function fields, and the especially its connection to the Tate conjecture. The following is the proposed lecture series, to be mostly presented by graduate students. The references I give below are not standard, but very accessible to beginners.

Lecture 1. *Introduction and organization*, Xinyi Yuan, Jan 28. I will sketch what are known over function fields, and outline the materials we will focus on. Then we will distribute the incoming weekly lectures to volunteers.

Lecture 2. *Statement of the full BSD conjecture.* The goal is to state the full BSD conjecture for elliptic curves over global fields. Define all the terms in the conjecture. In the case of elliptic curves over function fields, briefly recall the analytic property of the L-functions and the finiteness of the Mordell–Weil groups. Introduce what is known. Follow [Ul1, Lecture 1], except that the full BSD conjecture should be found in [Ul2, Conjecture 6.2.5].

Lecture 3. *Étale cohomology I: introduction.* It may takes one hour to even define étale cohomology (assuming everything in Hartshorne's book), but the purpose here is to convince us the existence of such a theory. Introduce three examples without proofs: (1) Identification with the usual (Zariski) sheaf cohomology when the étale sheaf is quasi-coherent. (2) Identification with Galois cohomology when the base is the spectrum of a field. (3) Interpretation of $H^1(S, G)$ as the group of G-torsors. Recommend [Po, Chap. 6] to beginners. See also [Mi1, Chap. 3].

Lecture 4. *Étale cohomology II: Weil conjecture.* Tell this fabulous story in one hour. State all the Weil's conjecture. Introduce ℓ-adic cohomology. Deduce the rationality of Weil's zeta function from it. Again, recommend [Po, Chap. 7] to beginners. See also [Mi1, VI.12].

Lecture 5. *Introduction to the Tate conjecture.* Present in the generality of any (smooth and projective) variety over finite fields. See [Mi2].

Lecture 6. *BSD vs Tate: rank part.* Explore the relation between both sides of the conjectures. For this lecture, only do the rank part. Give a full proof of [Ul1, Lecture 3, Thm. 8.1(1)].

Lecture 7. *BSD vs Tate: obstruction part.* Introduce the isomorphism between the Tate–Shafarevich group and the Brauer group. Two tasks in this hour: (1) Introduce spectral sequences. See [Po, §6.7] for example. (2). Sketch an idea of the proof, which should be less involved than [Ul2, §5.3.1], but should be complete assuming the fibration is everywhere smooth.

Lecture 8. *Brauer group of curves: class field theory.* Talk for the role of Brauer groups in both the local class field theory and the global class field theory. This is in fact a more basic topic, but it illustrates the significance of Brauer groups even in this one-dimensional case. See [CF, VI-VII].

Lecture 9. *Tate conjecture: homomorphisms between abelian varieties.* Introduce Tate's proof of his conjecture in this case. See [Ta].

Lecture 10. *Tate conjecture: K3 surfaces.* This case has been settled recently by the efforts of many people. Give an introduction. I will figured out which paper to focus on.

References

[CF] J.W.S. Cassels, A. Fröhlich, Algebraic Number Theory, (Eds), Algebraic Number Theory, Academic Press, 1967.

[Mi1] J. Milne, Lectures on Etale Cohomology, available at http://www.jmilne.org/math/CourseNotes/LEC.pdf.

[Mi2] J. Milne, The Tate conjecture over finite fields (AIM talk), available at http://www.jmilne.org/math/articles/2007e.pdf.

[Po] B. Poonen, Rational points on varieties, available at http://www-math.mit.edu/~poonen/papers/Qpoints.pdf.

[Ta] J. T. Tate. Endomorphisms of abelian varieties over finite fields. Invent. Math., 2: 134–144, 1966.

[Ul1] D. Ulmer, Elliptic curves over function fields, available at http://people.math.gatech.edu/~ulmer/research/papers/2011.pdf.

[Ul2] D. Ulmer, Curves and Jacobians over function fields, available at http://people.math.gatech.edu/~ulmer/research/papers/2014b.pdf.

26. Computing with Elliptic Curves over Number Fields Group, Lie and Number Theory Seminar University of Michigan, Ann Arbor, Michigan. January 20, 2015. 27. From the Diary of a Black Mathematician: My Journey from South Central to Studying Dessins dâ€™Enfants Marjorie Lee Browne Colloquium University of Michigan, Ann Arbor, Michigan.Â 56. Arithmetic Progressions on Curves Algebra/Combinatorics Seminar Texas A&M University, College Station, Texas. March 22, 2012. 57. Ellipses and Pendulums and Groups, Oh My!Â 118. Icosahedral Q-Curve Extensions Number Theory Seminar University of California, Irvine, California. April 2, 2002. 119. Icosahedral Q-Curve Extensions Number Theory Seminar University of California, Santa Barbara, California. Endomorphism rings of elliptic curves over nite elds. by. David Kohel Doctor of Philosophy in Mathematics.Â Theorem 2 There exists an algorithm that given a supersingular elliptic curve over a nite eld k computes four endomorphisms in O linearly independent over Z. For any Îµ > 0 the algorithm terminates deterministically in O(p2/3+Îµ) operations in the eld k and probabilistically with expected O(p1/2+Îµ) operations in k, where p is the characteristic of. The theory of elliptic curves is distinguished by its long history and by the diversity of the methods that have been used in its study. This book treats the arithmetic theory of elliptic curves in it.Â The theory of elliptic curves is distinguished by its long history and by the diversity of the methods that have been used in its study. This book treats the arithmetic theory of elliptic curves in its modern formulation, through the use of basic algebraic number theory and algebraic geometry. The book begins with a brief discussion of the necessary algebro-geometric results, and proceeds with an exposition of the geometry of elliptic curves, the formal group of an elliptic curve, and elliptic curves over finite fields, the complex numbers, local fields, and global fields. 2.2. Elliptic curves over local fields. 2.3. Selmer groups and Shafarevichâ€“Tate groups. 2.4. The Selmer group as an intersection of maximal isotropic direct summands.Â Our model will be inspired by theorems and con-jectures about the arithmetic of elliptic curves over Q. But before studying elliptic curves over Q, we should thoroughly understand elliptic curves over local elds. Let Qv be the completion of Q at a place v. There is a natural injective homomorphism inv : H2(Qv, Gm) â†’ Q/Z that is an isomorphism if v is nonarchimedean. Sage 9.1 Reference Manual: Curves Â». Elliptic curves over number fieldsÂ¶. An elliptic curve \(E\) over a number field \(K\) can be given by a Weierstrass equation whose coefficients lie in \(K\) or by using base_extend on an elliptic curve defined over a subfield.Â Another difference is the lack of understanding of modularity for general elliptic curves over general number fields. Currently Sage can obtain local information about \(E/K_v\) for finite places \(v\), it has an interface to Denis Simonâ€™s script for 2-descent, it can compute the torsion subgroup of the Mordell-Weil group \(E(K)\), and it can work with isogenies defined over \(K\).Â [Sil] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, 2009.