Elliptic curves over function fields 1

Douglas Ulmer

Georgia Institute of Technology

and

The University of Arizona
Arizona's First University

July 6, 2009

Goals for this lecture series:

- Explain old results of Tate and others on the BSD conjecture over function fields
- Show how certain classes of elliptic curves satisfy the BSD conjecture "*a priori*"
- Combine *a priori* BSD with analytic ranks results to obtain large rank Mordell-Weil groups
- Use related ideas to prove more and better cases of BSD and (time permitting) exhibit explicit points in high rank situations

Outline:

1. Basics on function fields and elliptic curves over function fields
2. Surfaces, the Tate conjecture, and Tate's theorem on products of curves
3. Elliptic surfaces and the connection between the Tate and BSD conjectures
4. Analytic ranks in towers of function fields
5. More BSD, a rank formula, and explicit points

What's omitted: Gross-Zagier. There is a (complicated, interesting) Drinfeld modular story in the function field case and a Gross-Zagier theorem, but we will not discuss it.

Function fields basics

k a field, usually finite.

K a finitely generated, regular extension of k of transcendence degree 1 (regular: K/k separable and k algebraically closed in K).

Key example: $k = \mathbb{F}_q$, $K = \mathbb{F}_q(t)$.

Exercise: Any k as above can be generated by two elements satisfying one relation. More precisely, $K \cong k(x)[y]/(f(x, y))$ for some irreducible $f \in k[x, y]$.

Associated to K there is a non-singular, projective curve C such that $K = k(C)$. It is unique up to k-isomorphism. We'll write g for its genus.

If $K = \mathbb{F}_q(t)$ then $C = \mathbb{P}^1_{\mathbb{F}_q}$.

In general, C is a non-singular, projective model of

$$\{f(x, y) = 0\} \subset \mathbb{A}^2.$$

Closed points of C correspond to places (equivalence classes of valuations) of K.

If $K = \mathbb{F}_q(t)$, the closed points of $C = \mathbb{P}^1$ correspond to $t = \infty$ and irreducible, monic polys in $\mathbb{F}_q[t]$.

For a closed point x write $\mathcal{O}_{(x)}$ for the valuation ring (functions defined near x), $\mathfrak{m}_x$ for the maximal ideal (functions vanishing at x) and $\kappa(x) = \mathcal{O}_{(x)}/\mathfrak{m}_x$ for the residue field at x (a finite extension of k).

Define $\deg(x) = [\kappa(x) : k]$. E.g., when $K = \mathbb{F}_q(t)$, $\deg(\infty) = 1$ and the degree of x corresponding to an irreducible f is $\deg(f)$.

Zetas

For $k = \mathbb{F}_q$, K/k as above, C the corresponding curve, define

$$Z(C,T) = \prod_{\text{closed } x} \left(1 - T^{\deg(x)}\right)^{-1} = \exp\left(\sum_{n\geq 1} N_n \frac{T^n}{n}\right).$$

Here N_n is the number of $\mathbb{F}_{q^n}$-valued points of C.

Exercise: Prove the second equality (for any variety over k). Hint: A closed point of C of degree d gives rise to exactly d $\mathbb{F}_{q^d}$-valued points .

Set $\zeta(C,s) = Z(C, q^{-s})$. This is a Dirichlet series in q^{-s} which converges in a half plane $\Re s > 1$.

Weil proved that $Z(C, T)$ is a rational function of the form

$$\frac{P_1(T)}{P_0(T)P_2(T)}$$

where $P_0(T) = (1 - T)$, $P_2(T) = (1 - qT)$, and

$$P_1(T) = 1 + \cdots + q^g T^{2g} = \prod_{i=1}^{2g}(1 - \alpha_i T)$$

where g is the genus of C and the α_i are algebraic integers with absolute value $q^{1/2}$ in any complex embedding.

Numbering the α_i suitably, we have $\alpha_{2g-i} = q/\alpha_i$.

It follows that $\zeta(C, s)$ has a meromorphic continuation to the whole s-plane with poles at $s = 0$ and $s = 1$, it satisfies a functional equation for $s \mapsto 1 - s$, and its zeroes lie on the line $\Re s = 1/2$.

Cohomology (lightning review)

Write $\overline{C}$ for $C \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ and note that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $\overline{C}$ via the $\overline{\mathbb{F}}_q$ factor.

Choose a prime ℓ not equal to the characteristic of k. Then we have cohomology groups $H^i(\overline{C}, \mathbb{Q}_\ell)$. These are finite-dimensional $\mathbb{Q}_\ell$-vector spaces with a continuous action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. They vanish unless $0 \leq i \leq 2 = 2\dim(C)$.

An important result is that

$$P_i(T) = \det(1 - T\,\mathrm{Fr}_q \,|H^i(\overline{C}, \mathbb{Q}_\ell))$$

where Fr_q is the geometric Frobenius ($a \mapsto a^{q^{-1}}$).

Note that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is generated topologically by Fr_q, so the Galois action is determined by that of Fr_q. Moreover, the action is known to be semi-simple in our case, so $P_i(T)$ determines $H^i(\overline{C}, \mathbb{Q}_\ell)$ with its Galois action, up to isomorphism.

Jacobians (lightning review)

The Jacobian J of C is a g-dimensional projective group variety defined over k. It classifies invertible sheaves (line bundles) on C, or equivalently, divisors up to linear equivalence.

Again let ℓ be a prime not equal to the characteristic of k. For $n \geq 1$, write $J[\ell^n]$ for the $\overline{\mathbb{F}}_q$ points of J of order ℓ^n. As a group this is $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. It also has a continuous, linear action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Form an inverse limit

$$T_\ell J = \operatorname{proj\,lim}_n J[\ell^n]$$

and set $V_\ell J = T_\ell J \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. $V_\ell J$ is a 2g-dimensional $\mathbb{Q}_\ell$-vector space with a continuous, linear action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ which is called the Tate module of J.

$V_\ell J$ was introduced by Weil as a substitute for cohomology (long before the $H^i(\overline{C}, \mathbb{Q}_\ell)$ were invented). The exercises sketch an argument showing that $V_\ell J = H_1(\overline{C}, \mathbb{Q}_\ell)$.

Elliptic curves over function fields: Definitions

As usual, an elliptic curve over K is a (non-singular, absolutely irreducible, projective) curve of genus 1 with a distinguished K-rational point.

We can always realize an elliptic curve E as a plane cubic with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the a_i are in K. We define b_i, c_i, Δ, and j by the usual formulas.

Conversely, a cubic equation as above with $\Delta \neq 0$ defines an elliptic curve where we take the point at infinity ($[0, 1, 0]$ in the usual coordinates) as the origin.

Constant and isotrivial

An elliptic curve over K/k is *constant* if it can be defined by a Weierstrass equation where the a_i are in k.

An elliptic curve E over K is *isotrivial* if there is a finite extension L of K such that E becomes constant over L. (More formally, if $E \times_K L \cong E_0 \times_k L$ where E_0 is an elliptic curve over k.)

For example ($p > 3$)

$$y^2 = x^3 + t^6$$

is constant and

$$y^2 = x^3 + t$$

is isotrivial.

Exercise: Show that E is isotrivial if and only if $j(E) \in k$.

Mordell-Weil

Given an elliptic curve E/K, the group of K-rational points $E(K)$ is called the Mordell-Weil group.

If E is not constant or if k is finitely generated over its prime field (e.g., k finite), then $E(K)$ is finitely generated (Mordell-Weil-Lang-Néron theorem).

One possible proof follows the same lines as when $K = \mathbb{Q}$: use descent arguments to show that $E(K)/nE(K)$ is finite and then use heights to show that $E(K)$ is finitely generated. We'll see another argument later using surfaces.

Reduction types

Let $E/K/k$ be as usual and choose a place x of K. It's always possible to choose a Weierstrass equation for E such that the a_i all lie in $\mathcal{O}_{(x)}$ and such that $\mathrm{ord}_x(\Delta)$ is minimal with respect to this condition.

Reducing the a_i modulo $\mathfrak{m}_x$ we get a plane cubic over $\kappa(x)$ which turns out to be independent of the choices up to isomorphism. If it is a smooth cubic, we say E has good reduction at x. If it is a nodal cubic we say E has multiplicative reduction (split or non-split according to the rationality of the tangents at the node) and if it is a cuspidal cubic, we say E has additive reduction.

Conductors

Assuming $p > 3$ for simplicity, we define the exponent of the conductor at x to be $\mathfrak{n}_x = 0$, 1, or 2 if E has good, multiplicative, or additive reduction. (The additive case is more complicated in small characteristics.)

The conductor is then the divisor $\mathfrak{n} = \sum_x \mathfrak{n}_x \cdot (x)$. Its degree is $\deg(\mathfrak{n}) = \sum_x \mathfrak{n}_x \deg(x)$.

Local factors

From now on, assume $k = \mathbb{F}_q$.

For each place x of K, let $q_x = \#\kappa(x)$. If E has good reduction at x, define a_x by

$$\#E(\kappa(x)) = q_x - a_x + 1.$$

Here the left hand side is the number of points on the reduced projective cubic rational over the residue field $\kappa(x)$.

If E has bad reduction a x, define $a_x = 1, -1, 0$ as E has split multiplicative, non-split multiplicative, or additive reduction at x. (There is a less ad hoc way to do this.)

By what was said before about zetas of curves over finite fields, if E has good reduction at x, the Z-function of E over $\kappa(x)$ is

$$\frac{1 - a_x T + q_x T^2}{(1 - T)(1 - qT)}$$

and in particular, $|a_x| \leq 2\sqrt{q_x}$.

L-functions

Define

$$Z(E,T) = \prod_{\text{good } x} (1 - a_x T + q_x T^2)^{-1} \prod_{\text{bad } x} (1 - a_x T)^{-1}$$

and $L(E,s) = Z(E, q^{-s})$.

Expanding in geometric series, $L(E,s)$ is a Dirichlet series in q^{-s} which converges for $\Re s > 3/2$.

Properties of $L(E, s)$

Hard theorems of Grothendieck, Raynaud, Deligne say:

- $L(E, s)$ is a rational function in q^{-s}.
- If E is not constant, $L(E, s)$ is a polynomial in q^{-s} of degree $4g_C - 4 + \deg(\mathfrak{n})$.
- $L(E, s)$ satisfies a functional equation for $s \mapsto 2 - s$.
- The zeroes of $L(E, s)$ lie on the line $\Re s = 1$.

BSD conjecture

The basic BSD conjecture says

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{Rank} E(K).$$

There is a refined conjecture expressing the leading coefficient of $L(E, s)$ near $s = 1$ in terms of heights, Tamagawa numbers (periods), and the order of $Ш(E/K)$. (So finiteness of $Ш$ is part of the refined conjecture.)

Main theorems I (Tate, Milne)

Let K be a function field over a finite field k of characteristic p and let E be an elliptic curve over K.

- Rank $E(K) \le \operatorname{ord}_{s=1} L(E,s)$
- Equality holds iff $\#Ш(E/K) < \infty$ iff $\#Ш(E/K)_{\ell^\infty} < \infty$ for any one ℓ ($\ell = p$ allowed).
- When equality holds, the refined BSD conjecture is true (on the nose, for any p).
- If L/K is a finite extension and BSD holds for E over L, then it holds for E over K.

Main theorems II

BSD holds for many special types of elliptic curves:

- (Tate) E constant. Thus also E isotrivial.
- (Tate, Milne, Artin-Swinnerton-Dyer) $K = \mathbb{F}_q(t)$ and E defined by a Weierstrass equation with $a_i \in \mathbb{F}_q[t]$ and $\deg(a_i) \leq 2i$.

Two more recent cases:

- (Ulmer, following Shioda) $K = \mathbb{F}_q(t)$ and E such that there exists a polynomial $g \in \mathbb{F}_q[t, x, y] \subset K[x, y]$ which is the sum of exactly 4 non-zero monomials with mild conditions on the exponents and such that $K(E) \cong K[x, y]/(g)$.
- (Berger) $K = \mathbb{F}_q(t)$ and E such that there exist separable rational functions $f(x)$, $g(y)$ on $\mathbb{P}^1_k$ with E the non-singular projective model of

$$V(f(x) - tg(y)) \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$$

  In this case (and the previous), BSD holds for E over $\mathbb{F}_q(t^{1/d})$ for all d prime to p.