Explicit points on the Legendre curve

Douglas Ulmer

Number Theory and Representation Theory
in honor of Dick Gross
June 2, 2010

Outline:

- Review of some results on ranks and the BSD conjecture for jacobians over function fields
- A completely explicit approach to high ranks

Analytic ranks theorem

$K = \mathbb{F}_q(t)$ with $q = p^f$, $K_d = \mathbb{F}_q(t^{1/d})$

A an abelian variety over K, $\mathfrak{n}$ the conductor of A, $\mathfrak{n}'$ the part prime to $t = 0$ and $t = \infty$.

Assume $\deg \mathfrak{n}' + \mathrm{Swan}_0(A) + \mathrm{Swan}_\infty(A)$ is odd.

Then $\mathrm{ord}_{s=1} L(A/K_d, s)$ is unbounded as d varies. More precisely, there is a $c = c(A)$ such that if $d = p^f + 1$,

$$\mathrm{ord}_{s=1} L(A/K_d, s) \geq \frac{d}{2f} - c.$$

For example, assume $p > 3$ and take for A an elliptic curve over $\mathbb{F}_q(t)$ with an odd number of places of multiplicative reduction away from 0 and ∞.

BSD and DPC (Tate)

A curve X over $K = \mathbb{F}_q(t)$ spreads out into a surface $\mathcal{X} \to \mathbb{P}^1$ over $\mathbb{F}_q$.

BSD for the Jacobian of X ($\operatorname{ord}_{s=1} L(J_X, s) = \operatorname{Rank} J(K)$) is equivalent to Tate for $\mathcal{X}$ ($-\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s) = \operatorname{Rank} NS(\mathcal{X})$).

Tate holds for a product of curves.

If Tate holds for $\mathcal{X}$ and $\mathcal{X} \dashrightarrow \mathcal{Y}$ is a dominant rational map, then Tate holds for $\mathcal{Y}$.

Upshot: If the surface $\mathcal{X}$ associated to X/K is DPC, then BSD holds for J_X.

DPCT

K_d/K is the generic fiber of $\mathbb{P}^1 \to \mathbb{P}^1$, $z \mapsto z^d$.

X/K_d spreads out to $\mathcal{X}_d$ sitting in a diagram:

$$\begin{array}{ccc} \mathcal{X}_d & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow[z \mapsto z^d]{} & \mathbb{P}^1 \end{array}$$

$\mathcal{X}$ DPC $\not\Rightarrow$ $\mathcal{X}_d$ DPC. We need "DPCT".

Get DPCT from "4 monomials" or from "Berger's construction".

4 monomials (Shioda)

Let X be a curve over $K = \mathbb{F}_q(t)$.

Assume X is birational to $\{g = 0\} \subset \mathbb{A}^2_K$ where $g \in \mathbb{F}_q[t, X, Y] \subset K[X, Y]$ is the sum of exactly 4 non-zero monomials (satisfying a mild condition on the exponents).

Thm: BSD holds for J_X.

(The 4-monomial condition implies that $\mathcal{X}$ is dominated by a Fermat surface, and Fermat surfaces are dominated by products of Fermat curves.)

Note that the condition is preserved under replacing t by u^d, i.e., we have DPCT.

Berger's construction (Berger)

Fix two curves $\mathcal{C}$ and $\mathcal{D}$ over $k = \mathbb{F}_q$ and non-constant, separable rational functions f on $\mathcal{C}$ and g on $\mathcal{D}$. Under mild conditions on f and g, there is a smooth proper model X of the curve

$$\{f - tg = 0\} \subset \mathcal{C} \times_k \mathcal{D} \times_k \operatorname{Spec} K$$

Thm: BSD holds for J_X over $\mathbb{F}_q(t^{1/d})$ for all d.

(The construction is set up so that $\mathcal{X}_d \to \mathbb{P}^1$ is dominated by $\mathcal{C}_d \times \mathcal{D}_d$ where $\mathcal{C}_d \to \mathcal{C}$ and $\mathcal{D}_d \to \mathcal{D}$ are obtained by extracting d-th roots of f and g.)

A rank formula

The Néron-Severi group of a product of curves is known in terms of Jacobians (Tate, Zarhin, Faltings) and this can be used to find NS of a surface dominated by a product of curves.

In Berger's context, this yields:

$$\operatorname{Rank} J_X(\overline{\mathbb{F}}_q(t^{1/d})) = \operatorname{Rank} \hom(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} - c_1(d) + c_2(d)$$

where c_1 is linear and c_2 is periodic.

(This works with $\mathbb{F}_q$ replaced by any field.)

Harvest

- For every p and every $g > 0$ there is a simple abelian variety of dimension g for which BSD holds and whose rank is as large as desired. (Analytic ranks + 4-monomials)
- Berger: There are *families* of elliptic curves over $\mathbb{F}_q(t)$ with BSD and unbounded rank in the tower $\mathbb{F}_q(t^{1/d})$. (Analytic ranks + Berger's construction)
- Occhipinti: There are elliptic curves over $\mathbb{F}_q(t)$ such that Rank $E(\overline{\mathbb{F}}_q(t^{1/d})) \geq d$ for *all* d prime to p. (Berger's construction and rank formula)
- There is an elliptic curve E over $\mathbb{F}_p(t)$ such that if $d = p^f + 1$ then Rank $E(\mathbb{F}_p(t^{1/d})) \sim p^f/2f$ and one can produce *explicit generators* for a finite index subgroup. (Rank formula and geometry of Berger's construction)

And now for something completely explicit ...

Legendre curve

$p > 2$, $K = \mathbb{F}_p(t)$, $K_d = \mathbb{F}_p(\mu_d)(u)$ with $u^d = t$.

$$E/K: \quad y^2 = x(x+1)(x+t)$$

Elementary exercise:

$$E(\mathbb{F}_p(u))_{tor} = E(\overline{\mathbb{F}}_p(u))_{tor} = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } d \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } d \text{ even} \end{cases}$$

$(Q = (u^{d/2}, u^{d/2}(u^{d/2}+1))$ is a 4-torsion point.)

Points

Assume until further notice that d has the form

$$d = p^f + 1 = q + 1.$$

Then $K_d = \mathbb{F}_{q^2}(t^{1/d}) = \mathbb{F}_{q^2}(u)$.

We have $P(u) = (u, u(u+1)^{(q+1)/2}) \in E(K_d)$

Apply Galois to get d points

$$P_i = P(\zeta_d^i u) \in E(K_d) \qquad i = 0, \ldots, d-1$$

Heights

Canonical heights on E are computable as intersection numbers on $\mathcal{E} \to \mathbb{P}^1$. Straightforward calculation yields:

$$\langle P_i, P_j \rangle = \begin{cases} \frac{(d-1)(d-2)}{2d} & \text{if } i = j \\ \frac{(1-d)}{d} & \text{if } i - j \text{ is even and } \neq 0 \\ 0 & \text{if } i - j \text{ is odd} \end{cases}$$

(We omit a factor of $\log q^2$.)

Corollaries: Rank $E(K_d) \geq d - 2 = q - 1$ and
Rank $E(\mathbb{F}_p(u)) \geq \sum_{e|d, e>2} \frac{\phi(e)}{o_e(p)} \sim q/2f$

BSD

Continuing to assume $d = q + 1$ ...

E/K_d has multiplicative reduction at 0, the d-th roots of unity, and ∞ (d is even), so $\deg_T L(E/K_d, T) = d - 2$. Because we have $d - 2 = q - 1$ independent points,

$$L(E/K_d, T) = (1 - q^2 T)^{(q-1)}.$$

Thus the rank inequalities of the last slide are equalities and BSD holds for E/K_d. In particular, $Ш(E/K_d)$ is finite.

Tate-Shafarevich group

Unwinding the BSD formula gives a beautiful expression for $|Ш(E/K_d)|$:

Let $V \subset E(K_d)$ be the subgroup generated by $P_0, \ldots, P_{d-1}$ and the torsion points. Then

$$|Ш(E/K_d)| = [E(K_d) : V]^2$$

Also, if $\mathbb{F}_r$ is an extension of $\mathbb{F}_{q^2}$, then

$$|Ш(E/\mathbb{F}_r(u)| = [E(K_d) : V]^2 \left(\frac{r}{q^2}\right)^{(q-1)/2}$$

This suggest that the p-Selmer group is linear in the ground field (as it will turn out to be).

Integrality

The height pairing is not in general integral, but its definition in terms of the (integral) intersection pairing on $\mathcal{E}$ gives a bound on denominator appearing in the regulator. Using this in the BSD formula gives a bound on $|Ш(E/K_d)|$:

$$\frac{q^{q-1}}{|Ш(E/K_d)|} \in \mathbb{Z}$$

So $|Ш(E/K_d)|$ and $[E(K_d) : V]$ are powers of p. We can test whether they are 1 by doing p-descent.

p-descent

Let A be the Hasse invariant of E (a polynomial of degree $(p-1)/2$ in t). Let $I_{p,d}$ be the curve over $\mathbb{F}_p$ which is the covering of $\mathbb{P}^1_u$ obtained by extracting a $(p-1)^{st}$ root of A. (I for Igusa.) Then

$$Sel(E/\mathbb{F}_r(u), p) = H^0(I_{p,d} \times \mathbb{F}_r, \Omega^1)^{\chi^{-1}, \mathcal{C}=0}$$

Here χ is the natural identification $\mathrm{Gal}(I_{p,d}/\mathbb{P}^1_u) \tilde{\to} {\mathbb{F}_p}^\times$ and $\mathcal{C}$ is the Cartier operator. Note that we get an $\mathbb{F}_r$ vector space, as expected.

Using this description, a crude analysis shows that $Ш(E/K_d) \neq 1$ whenever $f \geq p$. Explicit descents suggest that $Ш(E/K_d) \neq 1$ for all $f > 2$ and that $Ш(E/K_d) = 1$ often (always?) when $f = 1, 2$.

Connection with Berger

Now drop the assumption that $d = p^f + 1$: take d to be any positive integer prime to p.

E can be fit into the Berger construction—over an extension of K, E is isogenous to her X for $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$ and $f = x(x-1)$, $g = y^2/(1-y)$.

Consequences:

- Rank $E(\overline{\mathbb{Q}}(t^{1/d})) = 0$ for all d.
- BSD holds for E over $\mathbb{F}_r(t^{1/d})$ for all r and all d.

Rank formula for general d

Using the connection with Berger or elementary arguments, the L-function of E over K_d can be computed explicitly in terms of Jacobi sums for all d.

Stickelberger's theorem then gives a formula for the rank. Recall that $K_d = \mathbb{F}_p(\mu_d)(t^{1/d})$.

Let f be the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$ and for $t \in (\mathbb{Z}/d\mathbb{Z})^\times$ set

$$s_t = \sum_{j=0}^{f-1} 2\left\langle \frac{p^j}{d} \right\rangle + \left\langle \frac{-2p^j}{d} \right\rangle$$

This is an integer in $(0, 3f)$. Let

$$r_{p,d} = \begin{cases} \phi(d) & \text{if } s_t = 3f/2 \text{ for all } t \in (\mathbb{Z}/d\mathbb{Z})^\times \\ 0 & \text{otherwise} \end{cases}$$

Then we have

$$\operatorname{Rank} E(K_d) = \sum_{e|d, e>2} r_{p,e}$$

Interesting values of d

So, for example, if no power of p is $\equiv -1 \pmod{\ell}$, then Rank $E(K_d) = 0$ for $d = \ell^n$.

However, it turns out that there are many values of d for which $E(K_d)$ is large even when d is not a divisor of $p^f + 1$ for any f! (Thanks to Chris Hall for data supporting this assertion.)

E.g., suppose $d = 2(p^n - 1)$. One finds "new" rank at level d, i.e., $r_{p,d} = \phi(d)$. An explicit point which accounts for this rank is

$$(u^{-2}, u^{-3}(1 + u^2)^{(p^n+1)/2})$$

(Thanks to Ricardo Conceição for this point.)

The precise set of d for which there is new rank is mysterious.

Note that whether $r_{p,d}$ is zero or not depends only on p modulo d. Although there is a large literature on this question ("purity" of Gauss and Jacobi sums), apparently no simple characterization of pairs (p, d) for which $r_{p,d} \neq 0$ is known.

Generalizations

It is clear that the basic "trick" that makes the Legendre example work is quite general.

In particular, it will work in families and in higher genus. E.g., consider

$$y^2 = \prod_{i=1}^{g+1} (x + a_i)(a_i x + t)$$

where g is odd. It has obvious points over K_d for $d = q + 1$ whenever $a_i^q = a_i$.

Working out a general theory to encompass these examples looks like an interesting project.