Explicit points on elliptic curves of high rank over function fields

Douglas Ulmer
University of Arizona

Random matrices, L-functions, and primes
ETH, Zürich
October 27, 2008

Let p be a prime, $n \geq 1$, $q = p^n$, $d = p^n + 1$ and $k = \mathbb{F}_{q^2} = \mathbb{F}_p(\mu_d)$.

Let p be a prime, $n \geq 1$, $q = p^n$, $d = p^n + 1$ and $k = \mathbb{F}_{q^2} = \mathbb{F}_p(\mu_d)$.

Consider the elliptic curve

$$E: \qquad y^2 - xy + ty = x^3 - tx^2$$

over $k(t)$.

Let p be a prime, $n \geq 1$, $q = p^n$, $d = p^n + 1$ and $k = \mathbb{F}_{q^2} = \mathbb{F}_p(\mu_d)$.

Consider the elliptic curve

$$E : \qquad y^2 - xy + ty = x^3 - tx^2$$

over $k(t)$.

If $p > 2$, let

$$P(v) = (X(v), Y(v)) =$$

$$\left(\frac{v^q(v^q - v)}{1 + 4v^q}, \frac{1}{2}\left[\frac{v^{2q}}{(1+4v)^{q-1}} + \frac{v^{2q}(1 + 2v + 2v^q)}{(1+4v)^{(3q-1)/2}}\right]\right)$$

$$E: \qquad y^2 - txy + y = x^3 - tx^2$$

$$P(v) = \left(\frac{v^q(v^q - v)}{1 + 4v^q}, \frac{1}{2}\left[\frac{v^{2q}}{(1+4v)^{q-1}} + \frac{v^{2q}(1 + 2v + 2v^q)}{(1+4v)^{(3q-1)/2}} \right] \right)$$

Let $u = t^{1/d}$ and $K_d = k(u)$. Then for $i = 0, \ldots, d-1$

$$P(\zeta_d^i u) \in E(K_d),$$

they are almost independent (1 relation), and they generate a finite index subgroup of $E(K_d)$ which has rank $d-1$.

Goal is to explain a systematic construction of such examples.

Goal is to explain a systematic construction of such examples.

More elaborate examples have *parameters* (families!) so may be useful as a test bed for conjectures.

Goal is to explain a systematic construction of such examples.

More elaborate examples have *parameters* (families!) so may be useful as a test bed for conjectures.

Heights, regulators, Ш, ...

Goal is to explain a systematic construction of such examples.

More elaborate examples have *parameters* (families!) so may be useful as a test bed for conjectures.

Heights, regulators, Ш, ...

Engineering applications?

One can now produce ubiquitous examples of high analytic rank situations.

One can now produce ubiquitous examples of high analytic rank situations.

Roughly speaking, start with data (a curve, an abelian variety, ... a Galois representation) over $K = \mathbb{F}_q(t)$. If the data satisfies a mild parity condition, then the analytic rank of the L-function attached to the data over $K_d = \mathbb{F}_q(t^{1/d})$ will be unbounded as d varies.

One can now produce ubiquitous examples of high analytic rank situations.

Roughly speaking, start with data (a curve, an abelian variety, ... a Galois representation) over $K = \mathbb{F}_q(t)$. If the data satisfies a mild parity condition, then the analytic rank of the L-function attached to the data over $K_d = \mathbb{F}_q(t^{1/d})$ will be unbounded as d varies.

For example, if $p > 3$ and E is an elliptic curve over $\mathbb{F}_p(t)$ with an odd number of places of multiplicative reduction away from $t = 0$ and $t = \infty$, then $\operatorname{ord}_{s=1} L(E/K_d, s)$ is unbounded as d varies.

One can now produce ubiquitous examples of high analytic rank situations.

Roughly speaking, start with data (a curve, an abelian variety, ... a Galois representation) over $K = \mathbb{F}_q(t)$. If the data satisfies a mild parity condition, then the analytic rank of the L-function attached to the data over $K_d = \mathbb{F}_q(t^{1/d})$ will be unbounded as d varies.

For example, if $p > 3$ and E is an elliptic curve over $\mathbb{F}_p(t)$ with an odd number of places of multiplicative reduction away from $t = 0$ and $t = \infty$, then $\mathrm{ord}_{s=1} L(E/K_d, s)$ is unbounded as d varies.

Example:

$$y^2 = x^{2g+2} + x^{2g+1} + t$$

The BSD conjecture says $\text{ord}_{s=1} L(E/K_d, s) = \text{Rank}\, E(K_d)$. There are far fewer situations where one can prove this. Here is one:

The BSD conjecture says $\mathrm{ord}_{s=1} L(E/K_d, s) = \mathrm{Rank}\, E(K_d)$. There are far fewer situations where one can prove this. Here is one:

Theorem: Let X be a curve over $K = \mathbb{F}_q(t)$ and suppose there exists $g \in \mathbb{F}_q[t, x, y]$ which is the sum of exactly 4 non-zero monomials and such that $K(X) = \mathrm{Frac}\,(\mathbb{F}_q[t, x, y]/(g))$. Then under mild conditions on the exponents appearing in g, the BSD conjecture holds for $J = \mathrm{Jac}(X)$.

The BSD conjecture says $\mathrm{ord}_{s=1} L(E/K_d, s) = \mathrm{Rank}\, E(K_d)$. There are far fewer situations where one can prove this. Here is one:

Theorem: Let X be a curve over $K = \mathbb{F}_q(t)$ and suppose there exists $g \in \mathbb{F}_q[t, x, y]$ which is the sum of exactly 4 non-zero monomials and such that $K(X) = \mathrm{Frac}\,(\mathbb{F}_q[t, x, y]/(g))$. Then under mild conditions on the exponents appearing in g, the BSD conjecture holds for $J = \mathrm{Jac}(X)$.

This gives many examples of (simple, non-isotrivial) abelian varieties of every dimension with large rank.

Sketch of proof:

Curves/surfaces

Sketch of proof:

Curves/surfaces

points/divisors

Sketch of proof:

Curves/surfaces

points/divisors

L-functions/ζ-functions

Sketch of proof:

Curves/surfaces

points/divisors

L-functions/ζ-functions

BSD/Tate

Sketch continued:

4-monomials implies dominated by Fermat curves

Sketch continued:

4-monomials implies dominated by Fermat curves

Tate for products (for general k, good control on divisors on a product)

Sketch continued:

4-monomials implies dominated by Fermat curves

Tate for products (for general k, good control on divisors on a product)

Tate under dominant morphisms

Sketch continued:

4-monomials implies dominated by Fermat curves

Tate for products (for general k, good control on divisors on a product)

Tate under dominant morphisms

Put it all together

Remarks:

- 4-monomials is a stand-in for DPC

Remarks:

- 4-monomials is a stand-in for DPC

+ it is preserved in towers

Remarks:

• 4-monomials is a stand-in for DPC

+ it is preserved in towers

− it is very rigid

Remarks:

- 4-monomials is a stand-in for DPC

+ it is preserved in towers

− it is very rigid

Project: Find less rigid constructions of surfaces DPCT.

k arbitrary. $\mathcal{C}$, $\mathcal{D}$ curves over k. $f \in k(\mathcal{C})^\times$, $g \in k(\mathcal{D})^\times$.

k arbitrary. $\mathcal{C}$, $\mathcal{D}$ curves over k. $f \in k(\mathcal{C})^\times$, $g \in k(\mathcal{D})^\times$.

$\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1$ via $(x, y) \mapsto f(x)/g(y)$.

k arbitrary. $\mathcal{C}$, $\mathcal{D}$ curves over k. $f \in k(\mathcal{C})^\times$, $g \in k(\mathcal{D})^\times$.

$\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1$ via $(x, y) \mapsto f(x)/g(y)$.

Let X be the generic fiber, a curve over K.

k arbitrary. $\mathcal{C}$, $\mathcal{D}$ curves over k. $f \in k(\mathcal{C})^\times$, $g \in k(\mathcal{D})^\times$.

$\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1$ via $(x, y) \mapsto f(x)/g(y)$.

Let X be the generic fiber, a curve over K.

Associated surfaces $\mathcal{S}_d \to \mathbb{P}^1$ with generic fiber X/K_d.

k arbitrary. $\mathcal{C}$, $\mathcal{D}$ curves over k. $f \in k(\mathcal{C})^\times$, $g \in k(\mathcal{D})^\times$.

$\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1$ via $(x, y) \mapsto f(x)/g(y)$.

Let X be the generic fiber, a curve over K.

Associated surfaces $\mathcal{S}_d \to \mathbb{P}^1$ with generic fiber X/K_d.

Theorem (Berger, UA thesis 2007, JNT 2008): Under mild hypotheses on f and g,

- X is absolutely irreducible
- simple formula for genus of X
- $\mathcal{S}_d$ is DPC for all d

k arbitrary. $\mathcal{C}$, $\mathcal{D}$ curves over k. $f \in k(\mathcal{C})^\times$, $g \in k(\mathcal{D})^\times$.

$\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1$ via $(x, y) \mapsto f(x)/g(y)$.

Let X be the generic fiber, a curve over K.

Associated surfaces $\mathcal{S}_d \to \mathbb{P}^1$ with generic fiber X/K_d.

Theorem (Berger, UA thesis 2007, JNT 2008): Under mild hypotheses on f and g,

- X is absolutely irreducible
- simple formula for genus of X
- $\mathcal{S}_d$ is DPC for all d

Cor: For $k = \mathbb{F}_q$, there are families with parameters of elliptic curves over $\mathbb{F}_q(t)$ with arbitrarily large rank in the tower $\mathbb{F}_q(t^{1/d})$.

Back to k arbitrary.

Back to k arbitrary.

Berger's DPCT argument was based on π_1.

Back to k arbitrary.

Berger's DPCT argument was based on π_1.

But it can be made much more explicit:

$$\mathcal{C}_d : z^d = f(x) \qquad \mathcal{D}_d : w^d = g(y)$$

Back to k arbitrary.

Berger's DPCT argument was based on π_1.

But it can be made much more explicit:

$$\mathcal{C}_d : z^d = f(x) \qquad \mathcal{D}_d : w^d = g(y)$$

$$(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d \dashrightarrow \mathcal{S}_d$$

Working out the geometry leads to the following *rank formula* for $J = Jac(X)$:

$$\operatorname{Rank} J(K_d) = \operatorname{Rank} \hom_{k-av}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} - c_1 d + c_2$$

where c_1 is a constant and c_2 is periodic (usually constant).
($k = \overline{k}$ here, ...)

Working out the geometry leads to the following *rank formula* for $J = Jac(X)$:

$$\operatorname{Rank} J(K_d) = \operatorname{Rank} \hom_{k-av}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} - c_1 d + c_2$$

where c_1 is a constant and c_2 is periodic (usually constant). ($k = \overline{k}$ here, ...)

The numerical formula comes from a connection between homomorphisms and points which in good cases can be made very explicit.

Let $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$. Let $f(x) = x(x-1)$ and $g(y) = y^2/(y-1)$.

Let $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$. Let $f(x) = x(x-1)$ and $g(y) = y^2/(y-1)$.

It turns out that $X = E$ is the elliptic curve at the beginning. One finds $c_1 = c_2 = 0$

Let $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$. Let $f(x) = x(x-1)$ and $g(y) = y^2/(y-1)$.

It turns out that $X = E$ is the elliptic curve at the beginning. One finds $c_1 = c_2 = 0$

$\mathcal{C}_d \cong \mathcal{D}_d$ in a way that anti-commutes with μ_d actions. So,

$$\text{Rank}\, E(K_d) = \text{Rank}\, \text{End}_{k-av}(J_{\mathcal{C}_d})^{anti-\mu_d}$$

If k has characteristic zero, considering action of μ_d on 1-forms on X shows that Rank $E(K_d) = 0$ for all d.

If k has characteristic zero, considering action of μ_d on 1-forms on X shows that $\operatorname{Rank} E(K_d) = 0$ for all d.

If k is finite of characteristic p, let $d = p^n + 1$ and note that $Fr_{p^n} \circ \zeta_d = \zeta_d^{-1} \circ Fr_{p^n}$. Similarly,

$$(Fr_{p^n} \circ \zeta_d^i) \circ \zeta_d = \zeta_d^{-1} \circ (Fr_{p^n} \circ \zeta_d^i)$$

for all i. This gives many independent endomorphisms in $\operatorname{End}_{k-av}(J_{\mathcal{C}_d})^{anti-\mu_d}$. Tracing through the geometry leads to many independent points in $E(K_d)$.

Assume $k = \mathbb{C}$ for simplicity. Let $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$. Let $f(x) = x(x-a)/(x-1)$ and $g(y) = y(y-a)/(y-1)$. Here $a \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Assume $k = \mathbb{C}$ for simplicity. Let $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$. Let $f(x) = x(x-a)/(x-1)$ and $g(y) = y(y-a)/(y-1)$. Here $a \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

$X = E$ is again an elliptic curve. Let

$$S = \mathbb{P}^1 \setminus \{0, 1, \infty, -1, 1/2, 2, \zeta_6, \overline{\zeta}_6\}$$

For $a \in S$ one finds $c_1 = 1$, $c_2 = 4$ and

$$\operatorname{Rank} E(K_d) = \operatorname{Rank} \hom_{k-av}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} - d + 4.$$

Assume $k = \mathbb{C}$ for simplicity. Let $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$. Let $f(x) = x(x-a)/(x-1)$ and $g(y) = y(y-a)/(y-1)$. Here $a \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

$X = E$ is again an elliptic curve. Let

$$S = \mathbb{P}^1 \setminus \{0, 1, \infty, -1, 1/2, 2, \zeta_6, \overline{\zeta}_6\}$$

For $a \in S$ one finds $c_1 = 1$, $c_2 = 4$ and

$$\operatorname{Rank} E(K_d) = \operatorname{Rank} \hom_{k-av}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} - d + 4.$$

The term $-d$ cancels out the obvious endomorphisms $\zeta_d^i : J_{\mathcal{C}_d} \to J_{\mathcal{D}_d}$. To get rank we need some extra endomorphisms, i.e., CM.

Theorem: For

$$d \in \{2, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 24\}$$

there are infinitely many $a \in S$ such that

$$\mathrm{Rank}\, E(K_d) \geq \phi(d) + 3.$$

Theorem: For

$$d \in \{2, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 24\}$$

there are infinitely many $a \in S$ such that

$$\mathrm{Rank}\, E(K_d) \geq \phi(d) + 3.$$

Sketch: new/old, variation of Hodge structures, period domain is $(\mathcal{H})^r$.

Theorem: For

$$d \in \{2, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 24\}$$

there are infinitely many $a \in S$ such that

$$\operatorname{Rank} E(K_d) \geq \phi(d) + 3.$$

Sketch: new/old, variation of Hodge structures, period domain is $(\mathcal{H})^r$.

A-O: for fixed d only finitely many good a. But what about if d varies?