Diophantine Equations Counting Non-Ordinary Hyperelliptic Curves

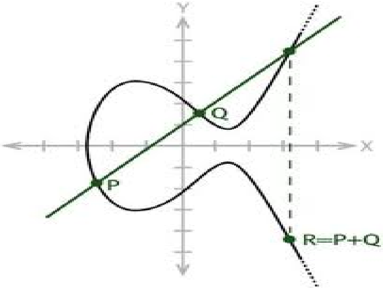
Colin Weir
The Tutte Institute for Mathematics and Computing

Joint work with
Derek Garton (Portland State)
Jeff Thunder (Northern Illinois)

West Coast Number Theory
December 2018

Elliptic Curves

- Let E be an elliptic curve over $k = \overline{\mathbb{F}_q}$, $q = p^n$.
- Then $E : y^2 = x^3 + ax^2 + bx + c = f(x)$ for $p > 2$.
- Algebraic groups law:



- $[\ell] : E \to E$ be mult. by ℓ morphism.
- The ℓ-torsion of E is $E[\ell] = Ker[\ell]$.

Computing the 3 torsion

Recall $E : y^2 = x^3 + ax^2 + bx + c$.

The case $\ell = 3$

$$3Q = Id \Leftrightarrow x(Q) \text{ is a root of the 3-division polynomial}$$

The 3-division polynomial is

$$\Psi_3(X) := 3X^4 + 4aX^3 + 6bX^2 + 12cX + 4ac - b^2$$

Computing the 3 torsion

Recall $E : y^2 = x^3 + ax^2 + bx + c$.

The case $\ell = 3$

$$3Q = Id \Leftrightarrow x(Q) \text{ is a root of the 3-division polynomial}$$

The 3-division polynomial is

$$\Psi_3(X) := 3X^4 + 4aX^3 + 6bX^2 + 12cX + 4ac - b^2$$

$p \neq 3$

$\Psi_3(X)$ has 4 roots, so $E[3](k) \cong (\mathbb{Z}/3)^2$.

Computing the 3 torsion

Recall $E : y^2 = x^3 + ax^2 + bx + c$.

The case $\ell = 3$

$$3Q = Id \Leftrightarrow x(Q) \text{ is a root of the 3-division polynomial}$$

The 3-division polynomial is

$$\Psi_3(X) := 3X^4 + 4aX^3 + 6bX^2 + 12cX + 4ac - b^2$$

$p \neq 3$

$\Psi_3(X)$ has 4 roots, so $E[3](k) \cong (\mathbb{Z}/3)^2$.

$p = 3$

$\Psi_3(X) = aX^3 + (ac - b^2)$

So $E[3](k) \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & a \neq 0, \quad \text{E is ordinary} \\ 1 & a = 0, \quad \text{E is supersingular} \end{cases}$

Higher Genus p-ranks of Curves

Let X be an hyperelliptic curve over k of genus g.
$X : y^2 = f(x)$, $deg(f(x)) = 2g + 2$, and $f(x)$ squarefree.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:
$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:

Higher Genus p-ranks of Curves

Let X be an hyperelliptic curve over k of genus g.
$X : y^2 = f(x)$, $deg(f(x)) = 2g + 2$, and $f(x)$ squarefree.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:
$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:
$J_X[p](k) \cong (\mathbb{Z}/p)^f$ for some $0 \leq f \leq g$. The value f is called the *p-rank* of X. X is ordinary if $f = g$

Higher Genus p-ranks of Curves

Let X be an hyperelliptic curve over k of genus g.
$X : y^2 = f(x)$, $deg(f(x)) = 2g + 2$, and $f(x)$ squarefree.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:
$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:
$J_X[p](k) \cong (\mathbb{Z}/p)^f$ for some $0 \leq f \leq g$. The value f is called the *p-rank* of X. X is ordinary if $f = g$

Does each p-rank actually occur? How often is a curve non-ordinary?

The a-number vs. The p-rank

The *p*-rank:

- Let μ_p be the kernel of F on $\mathbb{G}_m$.
- p-rank $f := \dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, J_X[p])$

The *a*-number

- Let α_p be the kernel of F on $\mathbb{G}_a$.
- a-number $a := \dim_{\mathbb{F}_p} \mathrm{Hom}(\alpha_p, J_X[p])$

$$\text{Fact: } 0 < a + f \leq g$$

Lemma

X non-ordinary if and only if $a > 0$

Computing the a-number

In General:

$$0 \to H^0(X, \Omega_1) \to H^1_{dR}(X) \to H^1(X, \mathcal{O}) \to 0$$

These spaces have dimensions

$$\dim(H^1_{dR}(X)) = 2g, \quad \dim(H^0(X, \Omega_1)) = g = \dim(H^1(X, \mathcal{O})).$$

Facts:

- $a = dim(\ker(F) \cap \ker(V))$
- $\ker(F) = H^0(X, \Omega_1)$
- $V|_{H^0(X,\Omega_1)}$ is the Cartier operator C
- Thus the a-number is the rank of the kernel of C

Random Matrix Theory

Heuristic: (Cais, Ellenberg, Zureick-Brown)

Rand .Mtx. Thy. predicts the following about (HE) Jacobians:

- a-number strata of (HE) Jacobians are irred. locally closed.
- Heuristic: $P(\text{ordinary}) = \prod_{j=1}^{\infty} \left(1 - q^{1-2j}\right)$

Also;

- They computed f & a of over a billion HE curves.
- The data they got agreed well with their heuristics (though not perfectly).
- Data: $P(\text{ordinary}) = \prod_{j=1}^{(p-1)/2} \left(1 - q^{1-2j}\right)$

In characteristic 3, data suggests there is a $1/q$ chance of being non-ordinary (as $g \to \infty$).

Computing Cartier and the a-number

Calculating the a-number

- $H^0(X, \Omega_1) = Span\{x^i \frac{dx}{y}\}_{i=0}^{g-1}$

The Cartier operator has the properties:

- $C(\omega_1 + \omega_2) = C(\omega_1) + C(\omega_2)$
- $C(z^p \omega) = zC(\omega)$
- $C(dz) = 0$
- $C(dz/z) = dz/z$

Making a Diophantine Problem (in Characteristic 3)

Write

$$f(x)^{\frac{p-1}{2}} = \sum_{j=0}^{p-1} x^j f_j(x^p)$$

then

$$C\left(x^i \frac{dx}{y}\right) = x^{\lfloor i/p \rfloor} f_{i \bmod p}(x) \frac{dx}{y}$$

In characteristic 3, counting non-ordinary hyperelliptic curves is counting 'low height' solutions $Z \in (k[x])^3$ to Diophantine equations of the form

$$Z_0 f_0(x) + Z_1 f_1(x) + Z_2 f_2(x) = 0.$$

The a-number = $\dim_k$(space of low height solutions).

Main Result

Theorem

In characteristic 3, the proportion of curves $y^2 = f(x)$*, with* $\deg(f(x)) = 2g + 2$ *and* $f(x)$ *cube-free with a-number* $a > A$ *is*

$$q^{-2A-1}$$

for any $A \geq g/3$*. No such curves have* $a > (g+2)/3$

Corollary

In characteristic 3, the proportion of non-ordinary curves $y^2 = f(x)$*, with* $\deg(f(x)) = 2g + 2$ *and* $f(x)$ *cube-free is* $1/q$*.*

Thank you