Rational points on curves and chip firing.

David Zureick-Brown (Emory University)
Eric Katz (Waterloo)

Slides available at `http://www.mathcs.emory.edu/~dzb/slides/`

2014 AMS special session
Arithmetic of Algebraic Curves
Knoxville, TN

March 22, 2014

Faltings' theorem

Theorem (Faltings)

Let X be a smooth curve over $\mathbb{Q}$ with genus at least 2. Then $X(\mathbb{Q})$ is finite.

Example

For $g \geq 2$, $y^2 = x^{2g+1} + 1$ has only finitely many solutions with $x, y \in \mathbb{Q}$.

Uniformity

Problem

1. *Given X, compute $X(\mathbb{Q})$ exactly.*
2. *Compute bounds on $\#X(\mathbb{Q})$.*

Conjecture (Uniformity)

There exists a constant $N(g)$ such that every smooth curve of genus g over $\mathbb{Q}$ has at most $N(g)$ rational points.

This would follow from standard conjectures (e.g. Lang's conjecture, the higher dimensional analogue of Faltings' theorem).

Coleman's bound

Theorem (Coleman)

Let X be a curve of genus g and let $r = \mathrm{rank}_{\mathbb{Z}} \mathrm{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime of good reduction. Suppose $r < g$. Then

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

Remark

1. A modified statement holds for $p \leq 2g$ or for $K \neq \mathbb{Q}$.
2. Note: this does not prove uniformity (since the first good p might be large).

Stoll's bound

Theorem (Stoll)

Let X be a curve of genus g and let $r = \operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime of good reduction. Suppose $r < g$. Then

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r.$$

Bad reduction bound

Theorem (Lorenzini-Tucker, McCallum-Poonen)

Let X be a curve of genus g and let $r = \mathrm{rank}_{\mathbb{Z}} \mathrm{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime. Suppose $r < g$.

Let $\mathscr{X}$ be a regular proper model of X. *Then*

$$\#X(\mathbb{Q}) \leq \#\mathscr{X}^{\mathrm{sm}}(\mathbb{F}_p) + 2g - 2.$$

Remark

A recent improvement due to Stoll gives a uniform bound if $r \leq g - 3$ and X is hyperelliptic.

Main Theorem

Theorem (Katz-ZB)

Let X be a curve of genus g and let $r = \operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime. Let $\mathscr{X}$ be a regular proper model of X. Suppose $r < g$. Then

$$\#X(\mathbb{Q}) \leq \#\mathscr{X}^{\mathrm{sm}}(\mathbb{F}_p) + 2r.$$

Example (hyperelliptic curve with cuspidal reduction)

$$
\begin{aligned}
-2 \cdot 11 \cdot 19 \cdot 173 \cdot y^2 &= (x-50)(x-9)(x-3)(x+13)(x^3+2x^2+3x+4) \\
&= x(x+1)(x+2)(x+3)(x+4)^3 \quad \bmod 5.
\end{aligned}
$$

Analysis

1. $X(\mathbb{Q})$ contains

$$\{\infty, (50,0), (9,0), (3,0), (-13,0), (25, 20247920), (25, -20247920)\}$$

2. $\#\mathscr{X}_5^{\mathrm{sm}}(\mathbb{F}_5) = 5$
3. $7 \leq \#X(\mathbb{Q}) \leq \#\mathscr{X}_5^{\mathrm{sm}}(\mathbb{F}_5) + 2 \cdot 1 = 7$

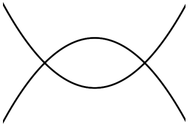
This determines $X(\mathbb{Q})$.

Non-example

$$\begin{aligned} y^2 &= x^6 + 5 \\ &= x^6 \mod 5. \end{aligned}$$

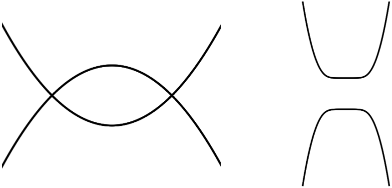
Analysis

1. $X(\mathbb{Q}) \supset \{\infty^+, \infty^-\}$
2. $\mathscr{X}^{\mathrm{sm}}(\mathbb{F}_5) = \{\infty^+, \infty^-, \pm(1, \pm 1), \pm(2, \pm 2^3), \pm(3, \pm 3^3), \pm(4, \pm 4^3)\}$
3. $2 \leq \#X(\mathbb{Q}) \leq \#\mathscr{X}_5^{\mathrm{sm}}(\mathbb{F}_5) + 2 \cdot 1 = 20$



Models

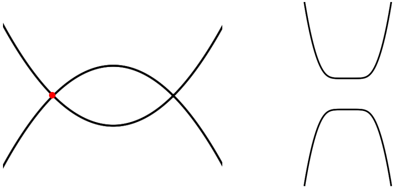
$$\begin{aligned} y^2 &= x^6 + 5 \\ &= x^6 \mod 5. \end{aligned}$$



Note: no point can reduce to $(0,0)$.

Models

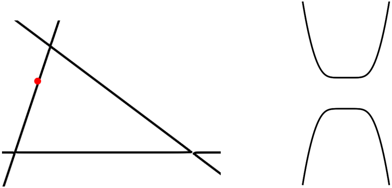
$$
\begin{aligned}
y^2 &= x^6 + 5^{\color{red}2} \\
&= x^6 \mod 5
\end{aligned}
$$



Now: $(0,5)$ reduces to $(0,0)$. Local equation looks like $xy = 5^2$

Models

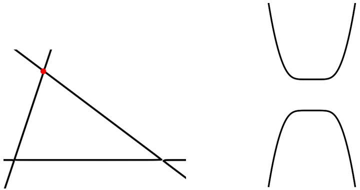
$$\begin{aligned} y^2 &= x^6 + 5^2 \\ &= x^6 \mod 5 \end{aligned}$$



Blow up. Local equation looks like $xy = 5$

Models

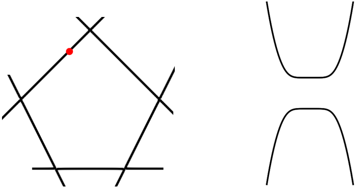
$$\begin{aligned} y^2 &= x^6 + 5^{4} \\ &= x^6 \mod 5 \end{aligned}$$



Blow up. Local equation looks like $xy = 5^3$

Models

$$
\begin{aligned}
y^2 &= x^6 + 5^{4} \\
&= x^6 \mod 5
\end{aligned}
$$



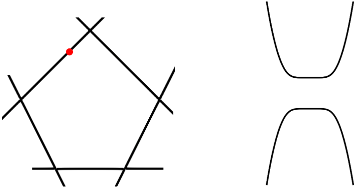
Blow up. Local equation looks like $xy = 5$

Main Theorem

Theorem (Katz-ZB)

Let X be a curve of genus g and let $r = \operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime. Let $\mathscr{X}$ be a regular proper model of X. Suppose $r < g$. Then

$$\#X(\mathbb{Q}) \leq \#\mathscr{X}^{\mathrm{sm}}(\mathbb{F}_p) + 2r.$$



Chabauty's method

(*p*-**adic integration**) There exists $V \subset H^0(X_{\mathbb{Q}_p}, \Omega^1_X)$ with $\dim_{\mathbb{Q}_p} V \geq g - r$ such that,

$$\int_P^Q \omega = 0 \qquad \forall P, Q \in X(\mathbb{Q}), \omega \in V$$

(**Coleman, via Newton Polygons**) Number of zeroes in a residue disc D_P is $\leq 1 + n_P$, where $n_P = \#\left(\operatorname{div}\omega \cap D_P\right)$

(**Riemann-Roch**) $\sum n_P = 2g - 2$.

(**Coleman's bound**) $\sum_{P \in X(\mathbb{F}_p)} (1 + n_P) = \#X(\mathbb{F}_p) + 2g - 2$.

Example (from McCallum-Poonen's survey paper)

Example

$$X\colon y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$$

1. Points reducing to $\widetilde{Q} = (0,1)$ are given by

$$\begin{aligned} x &= \; p \cdot t, \text{ where } t \in \mathbb{Z}_p \\ y &= \; \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} = 1 + x^2 + \cdots \end{aligned}$$

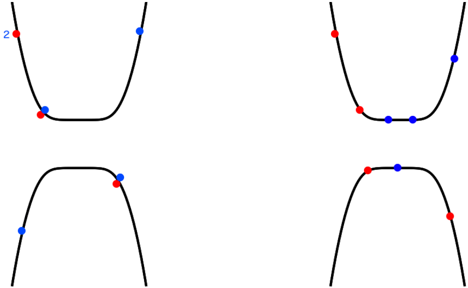
2. $\displaystyle\int_{(0,1)}^{P_t} \frac{xdx}{y} = \int_0^t (x - x^3 + \cdots)dx$

Stoll's idea: use multiple ω

(**Coleman, via Newton Polygons**) Number of zeroes of $\int \omega$ in a residue class D_P is $\leq 1 + n_P$, where $n_P = \#(\operatorname{div}\omega \cap D_P)$

Let $\widetilde{n_P} = \min_{\omega \in V} \#(\operatorname{div}\omega \cap D_P)$

(**Example**) $r \leq g - 2$, ω_1, $\omega_2 \in V$



(**Stoll's bound**) $\sum \widetilde{n_P} \leq 2r$. (Recall $\dim_{\mathbb{Q}_p} V \geq g - r$)

Stoll's bound; proof.

Let $D = \sum \widetilde{n_P} P$. Wanted: $\deg D \leq 2r$

(Clifford) If $H^0(X_{\mathbb{F}_p}, K - D') \neq 0$ then

$$\dim H^0(X_{\mathbb{F}_p}, D') \leq \frac{1}{2} \deg D' + 1$$

$\mathbf{(}D' = K - D\mathbf{)}$

$$\frac{1}{2} \deg(K - D) + 1 \geq \dim H^0(X_{\mathbb{F}_p}, K - D)$$

(**Assumption**)

$$\dim H^0(X_{\mathbb{F}_p}, K - D) \geq g - r$$

(Recall $\dim_{\mathbb{Q}_p} V \geq g - r$)

Complications when $X_{\mathbb{F}_p}$ is singular

1. $\omega \in H^0(X, \Omega)$ may vanish along components of $X_{\mathbb{F}_p}$.
2. I.e. $H^0(X_{\mathbb{F}_p}, K - D) \neq 0 \not\Rightarrow D$ is special.
3. $\operatorname{rank}(K - D) \neq \dim H^0(X_{\mathbb{F}_p}, K - D) - 1$

Summary

The relationship between $\dim H^0(X_{\mathbb{F}_p}, K - D)$ and $\deg D$ is less transparent and does not follow from geometric techniques.

Rank of a divisor

Definition (Rank of a divisor is)

1. $r(D) = -1$ if $|D|$ is empty.
2. $r(D) \geq 0$ if $|D|$ is nonempty
3. $r(D) \geq k$ if $|D - E|$ is nonempty for any effective E with $\deg E = k$.

Remark

1. If X is smooth, then $r(D) = \dim H^0(X, D) - 1$.
2. If X is has multiple components, then $r(D) \neq \dim H^0(X, D) - 1$.

Remark

Ingredients of Stoll's proof only use formal properties of $r(D)$.

Formal ingredients of Stoll's proof

Need:

$$\text{(Clifford)} \quad r(K-D) \leq \tfrac{1}{2}\deg(K-D)$$

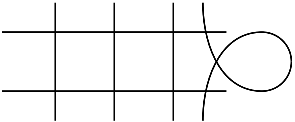
$$\text{(Large rank)} \quad r(K-D) \geq g-r-1$$

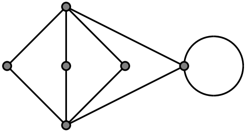
(Recall, $V \subset H^0(X_{\mathbb{Q}_p}, \Omega^1_X), \dim_{\mathbb{Q}_p} V \geq g-r$)

Semistable case

Idea: any section $s \in H^0(X, D)$ can be scaled to not vanish on a component (but may now have zeroes or poles at other components.)

Divisors on graphs:

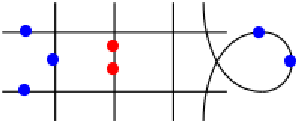


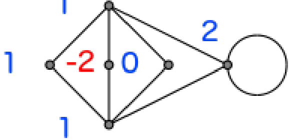


Semistable case

Idea: any section $s \in H^0(X, D)$ can be scaled to not vanish on a component (but may now have zeroes or poles at other components.)

Divisors on graphs:

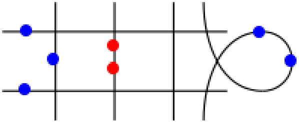


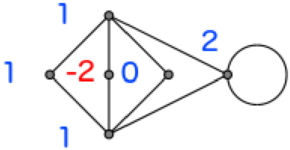


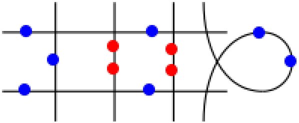
Semistable case

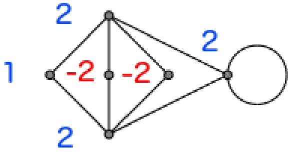
Idea: any section $s \in H^0(X, D)$ can be scaled to not vanish on a component (but may now have zeroes or poles at other components.)

Divisors on graphs:





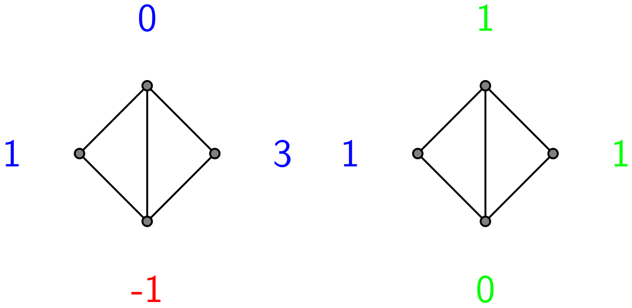




Divisors on graphs

Definition (Rank of a divisor is)

1. $r(D) = -1$ if $|D|$ is empty.
2. $r(D) \geq 0$ if $|D|$ is nonempty
3. $r(D) \geq k$ if $|D - E|$ is nonempty for any effective E with $\deg E = k$.

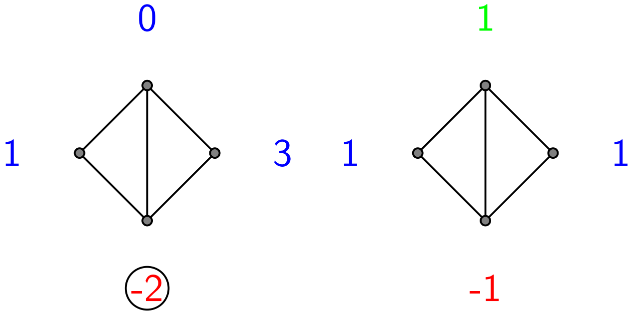


Remark

$r(D) \geq 0$

Definition (Rank of a divisor is)

1. $r(D) = -1$ if $|D|$ is empty.
2. $r(D) \geq 0$ if $|D|$ is nonempty
3. $r(D) \geq k$ if $|D - E|$ is nonempty for any effective E with $\deg E = k$.



Remark

$r(D) \geq 1$

Divisors on graphs

Definition

For $\overline{D} \in \operatorname{Div}\Gamma$, $r_{\text{num}}(\overline{D}) \geq k$ if $|\overline{D} - \overline{E}|$ is non-empty for every effective $\overline{E}$ of degree k.

Theorem (Baker, Norine)

Riemann-Roch *for r_{num}.*

Clifford's theorem *for r_{num}.*

Specialization*: $r_{num}(\overline{D}) \geq r(D)$.*

Formal corollary*: $X(\mathbb{Q}) \leq \#X^{\text{sm}}(\mathbb{F}_p) + 2r$ (for X totally degenerate).*

General case (not totally degenerate) – abelian rank

Problems when $g(\Gamma) < g(X)$. (E.g. rank can increase after reduction.)

Definition (Abelian rank r_{ab})

After winning winning the chip firing game, we additionally require that the resulting divisor is equivalent to an effective divisor on that component.

Theorem (Katz-ZB)

- **Clifford's theorem**: *for* r_{ab}
- **Specialization**: $r_{\mathrm{ab}}(K - D) \geq g - r$.
- **Formal corollary**: $X(\mathbb{Q}) \leq \#X^{\mathrm{sm}}(\mathbb{F}_p) + 2r$ *(for semistable curves.)*