Rational points on curves and tropical geometry.

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

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

Specialization of Linear Series for Algebraic and Tropical Curves
BIRS

April 3, 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.

Theorem (Caporaso, Harris, Mazur)

Lang's conjecture $\Rightarrow$ uniformity.

Coleman's bound

Theorem (Coleman)

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

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

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

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

Bad reduction bound

Theorem (Lorenzini-Tucker, McCallum-Poonen)

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. 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)

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

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

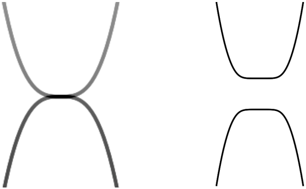
This determines $X(\mathbb{Q})$.

Non-example

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

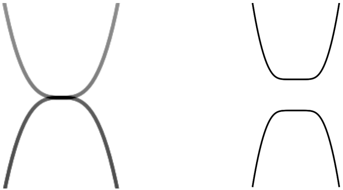
Analysis

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 ($\mathscr{X}/\mathbb{Z}_p$)

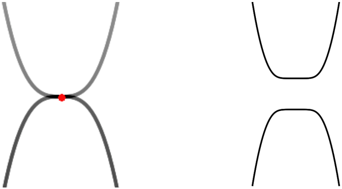
$$\begin{aligned} y^2 &= x^6 + 5 \\ &= x^6 \mod 5. \end{aligned}$$



Note: no $\mathbb{Z}_p$-point can reduce to $(0,0)$.

Models – not regular

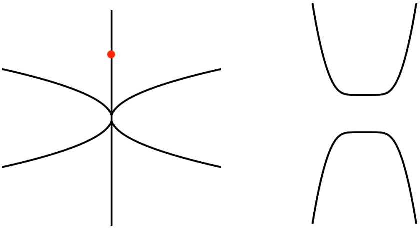
$$\begin{aligned} y^2 &= x^6 + 5^{2} \\ &= x^6 \mod 5 \end{aligned}$$



Now: $(0,5)$ reduces to $(0,0)$.

Models – not regular (blow up)

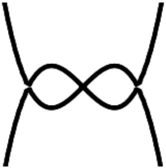
$$\begin{aligned} y^2 &= x^6 + 5^{2} \\ &= x^6 \mod 5 \end{aligned}$$

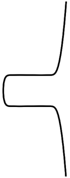


Blow up.

Models – semistable example

$$\begin{aligned} y^2 &= (x(x-1)(x-2))^3 + 5 \\ &= x^6 \mod 5. \end{aligned}$$

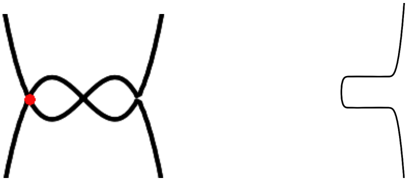




Note: no point can reduce to $(0,0)$. Local equation looks like $xy = 5$

Models – semistable example (not regular)

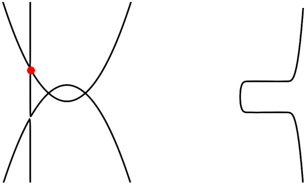
$$y^2 = (x(x-1)(x-2))^3 + 5^{4}$$
$$= x^6 \mod 5$$



Now: $(0, 5^2)$ reduces to $(0, 0)$. Local equation looks like $xy = 5^4$

Models – semistable example

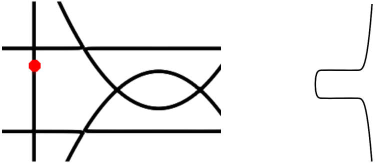
$$\begin{aligned} y^2 &= (x(x-1)(x-2))^3 + 5^{4} \\ &= x^6 \mod 5 \end{aligned}$$



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

Models – semistable example (regular at (0,0))

$$
\begin{aligned}
y^2 &= (x(x-1)(x-2))^3 + 5^{\color{red}4} \\
&= x^6 \mod 5
\end{aligned}
$$



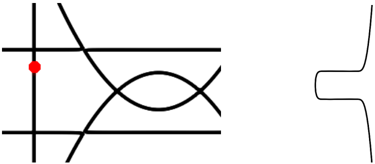
Blow up. Local equation looks like $xy = 5$

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

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



(**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

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

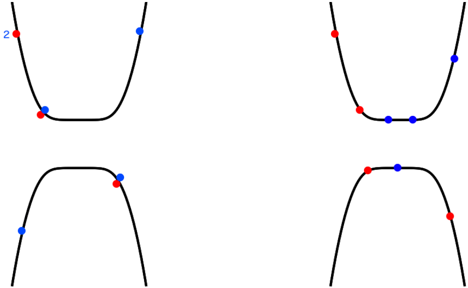
2. $\displaystyle\int_{(0,1)}^{P_t} \frac{xdx}{y} = \int_0^t (x - x^3 + \cdots)dx$

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 $n_P = \#\left(\operatorname{div}\omega \cap D_P\right)$

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

(**2 examples**) $r \leq g - 2$, 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 ($D = \sum \widetilde{n_P} P$)

(Wanted)

$$\dim H^0(X_{\mathbb{F}_p}, K - D) \geq g - r \Rightarrow \deg D \leq 2r$$

(Clifford)

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

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

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

(**Assumption**)

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

(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. $\mathrm{rank}(K - D) \neq \dim H^0(X_{\mathbb{F}_p}, K - D) - 1$

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:

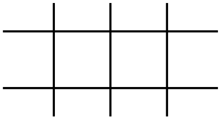
$$\text{(Clifford)} \quad r(K-D) \leq \tfrac{1}{2}\deg(K-D)$$

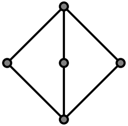
$$\text{(Large rank)} \quad r(K-D) \geq g-r-1$$

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

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.)

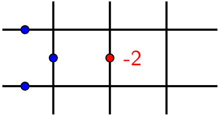
Divisors on graphs:

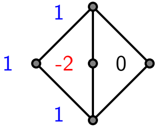




Idea: any section $s \in H^0(X, D)$ can be scaled to not vanish on a component (but may now have zeroes or poles at other components.)

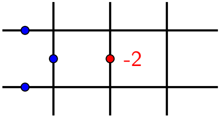
Divisors on graphs:

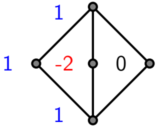


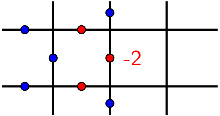


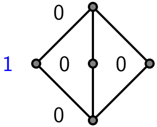
Idea: any section $s \in H^0(X, D)$ can be scaled to not vanish on a component (but may now have zeroes or poles at other components.)

Divisors on graphs:



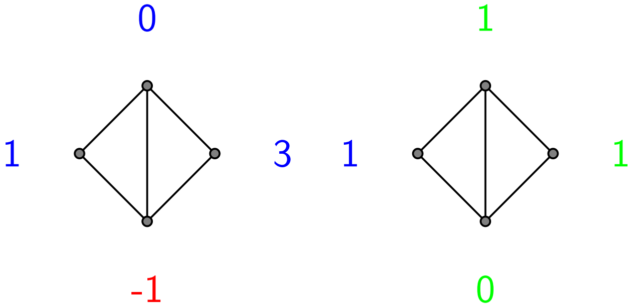






Definition (Rank of a divisor is)

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 $\deg E = k$.



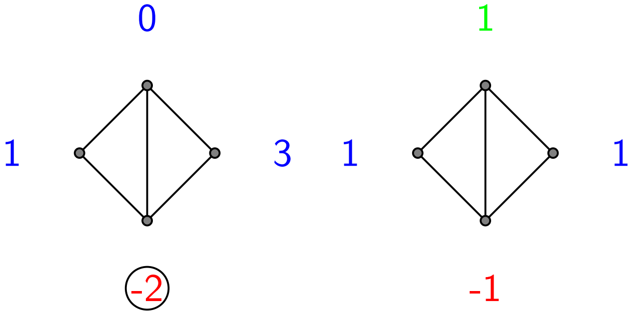
Remark

$r(D) \geq 0$

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

$r(D) \geq 1$

Semistable case – line bundles

Let $\mathscr{X}$ be a curve over $\mathbb{Z}_p$ with semistable special fiber $\mathscr{X}_{\mathbb{F}_p} = \bigcup X_i$.

Definition (Divisor associated to a line bundle)

Given $\mathcal{L} \in \operatorname{Pic} \mathscr{X}$, define a divisor on Γ by

$$\sum_{v \in V(\Gamma)} (\deg \mathcal{L}_{X_i}) v_{X_i}.$$

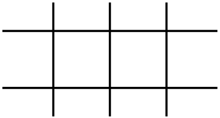
Let $\mathscr{X}$ be a curve over $\mathbb{Z}_p$ with semistable special fiber $\mathscr{X}_{\mathbb{F}_p} = \bigcup X_i$.

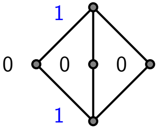
Definition (Divisor associated to a line bundle)

Given $\mathcal{L} \in \operatorname{Pic} \mathscr{X}$, define a divisor on Γ by

$$\sum_{v \in V(\Gamma)} (\deg \mathcal{L}_{X_i}) v_{X_i}.$$

Example: $\mathcal{L} = \omega_{\mathscr{X}}$, $\mathscr{X}_{\mathbb{F}_p}$ totally degenerate ($g(X_i) = 0$)





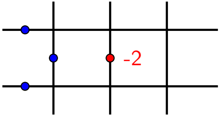
Let $\mathscr{X}$ be a curve over $\mathbb{Z}_p$ with semistable special fiber $\mathscr{X}_{\mathbb{F}_p} = \bigcup X_i$.

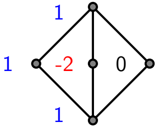
Definition (Divisor associated to a line bundle)

Given $\mathcal{L} \in \operatorname{Pic} \mathscr{X}$, define a divisor on Γ by

$$\sum_{v \in V(\Gamma)} (\deg \mathcal{L}_{X_i}) v_{X_i}.$$

Example: $\mathcal{L} = \mathcal{O}(H)$ (H a "horizontal" divisor on $\mathscr{X}$)





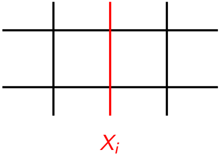
Let $\mathscr{X}$ be a curve over $\mathbb{Z}_p$ with semistable special fiber $\mathscr{X}_{\mathbb{F}_p} = \bigcup X_i$.

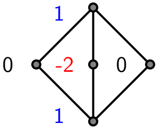
Definition (Divisor associated to a line bundle)

Given $\mathcal{L} \in \operatorname{Pic} \mathscr{X}$, define a divisor on Γ by

$$\sum_{v \in V(\Gamma)} (\deg \mathcal{L}_{X_i}) v_{X_i}.$$

Example: $\mathcal{L} = \mathcal{O}(X_i)$,



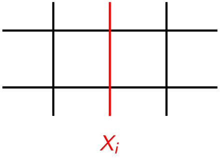


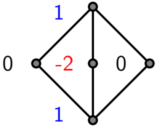
Definition

For $\overline{D} \in \operatorname{Div}\Gamma$, $r_{\mathrm{num}}(\overline{D}) \geq k$ 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**: $X(\mathbb{Q}) \leq \#\mathscr{X}^{\mathrm{sm}}(\mathbb{F}_p) + 2r$ *(for* X *totally degenerate).*





Remark (Main points)

1. Chip firing is the same as twising by $\mathcal{O}(X_i)$.
2. If $\exists s \in H^0(\mathscr{X}, \mathcal{L})$ and $\operatorname{div} s = \sum H_i + \sum n_i X_i$, then

$$\mathcal{L} \otimes \mathcal{O}(-n_1 X_1) \otimes \cdots \otimes \mathcal{O}(-n_k X_k)$$

   specializes to an effective divisor on Γ.
3. The firing sequence $(n_1, \ldots, n_n)$ wins the chip firing game.

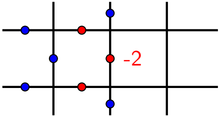
Semistable but not totally degenerate – abelian rank

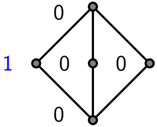
Problems when $g(\Gamma) < g(X)$. (E.g. rank can increase after reduction.)

Definition (Abelian rank r_{ab})

Let $\mathcal{L} \in \mathcal{X}$ have specialization $D \in \operatorname{Div}\Gamma$. Then $r_{\mathrm{ab}}(\mathcal{L}) \geq k$ if

1. $|D - E|$ is nonempty for any effective E with $\deg E = k$, and
2. for every $\mathcal{L}_E$ specializing to E, there exists some $(n_1, \ldots, n_k)$ such that
$$\mathcal{L}' := \mathcal{L} \otimes \mathcal{L}_E^{-1} \otimes \mathcal{O}(n_1 X_1) \otimes \cdots \otimes \mathcal{O}(n_k X_k)$$
has effective specialization and such that $H^0(X_i, \mathcal{L}'_{X_i}) \neq 0$ for every component X_i.





Main Theorem – abelian rank

Theorem (Katz-ZB)

Clifford's theorem: $r_{\mathrm{ab}}(K - D) \leq \frac{1}{2}\deg(K - D)$

Specialization: $r_{\mathrm{ab}}(K - D) \geq g - r$.

Formal corollary: $X(\mathbb{Q}) \leq \#\mathscr{X}^{\mathrm{sm}}(\mathbb{F}_p) + 2r$ *(for semistable curves.)*

Final remarks

Remark

Also prove: **semistable case** $\Rightarrow$ **general case**.

Remark (Néron models)

1. Suppose $\mathcal{L} \in \mathrm{Pic}_{\mathscr{X}}$ and $\deg\left(\mathcal{L}|_{\mathscr{X}_p}\right) = 0$.
2. $r_{\mathrm{num}}(\mathcal{L}) = 0$ if and only if $\mathcal{L}|_{\mathscr{X}_p} \in \mathrm{Pic}^0_{\mathscr{X}_p}$.
3. $r_{\mathrm{ab}}(\mathcal{L}) = 0$ if and only if the image of $\mathcal{L}|_{\mathscr{X}_p}$ in $\mathrm{Pic}^0_{\widetilde{\mathscr{X}_p}}$ is the identity.

Remark (Toric rank)

1. Can also define r_{tor} – additionally require that sections agree at nodes
2. r_{tor} incorporates the toric part of Néron model