# $p$-adic heights and integral points on curves

Amnon Besser

24/7/2018

# Goal

Explain how $p$-adic heights can be used to find integral points on curves.

This is related but independent of Kim's program.

Emphasis is on algorithms for finding points rather than on proving finiteness.

# Plan

- A theorem of Kim
- General theory of $p$-adic height pairings
- The Coleman-Gross $p$-adic height pairing.
- Divisors with non-disjoint supports.
- Quadratic Chabauty for elliptic curves
- Quadratic Chabauty for hyperelliptic curves
- Number fields
- The Mordell-Weil Sieve

# Kim's Theorem

Let $E/\mathbb{Q}$ be an elliptic curve, in minimal model $y^2 = f(x)$, with the following properties

- $\mathrm{rank}(E) = 1$
- $p$ is a good reduction prime s.t. the $p$-part of the Tate-Shafarevich group of $E$ is finite
- At each bad reduction prime the Néron model has just one component.

# Kim's Theorem

**Theorem (Kim, + Balakrishnan, Kedlaya, Kim)**

*There exists an explicit Coleman integral $\tau$ on $E(\mathbb{Q}_p)$ such that $\tau(P)/(\int_0^P \omega)^2$ is constant on integral points, where $\omega = \frac{dx}{2y}$ is the invariant differential and*

$$\tau(P) = \int(\omega \times \int \bar{\omega}), \quad \bar{\omega} = \frac{xdx}{2y}$$

# The Nekovar height pairing

Nekovar (1993) defines a (Galois theoretic) bilinear $p$-adic height pairing

$$H^1_f(F, V) \times H^1_f(F, V^*(1)) \to \mathbb{Q}_p$$

- $V$ - a $G = \mathrm{Gal}(\bar{F}/F)$ $p$-adic representation satisfying certain conditions, e.g. $V = H^1_{\text{ét}}(\bar{X}, \mathbb{Q}_p(1))$, $\dim(X) = 1$.
- $H_f$ - finite cohomology (recalled below)

In geometric situation one gets a pairing on cycles using the $p$-adic Abel-Jacobi map, e.g., for deg 0 divisors on a curve $X$.

$$\alpha : \mathrm{Div}_0(X) \to J(F) \xrightarrow{\text{Kummer}} H^1_f(F, T_p(J)) \quad , J = J_X$$

# Finite cohomology

$V$ a $p$-adic representation of $G$, crystalline at primes above $p$.

$v \nmid p$ - $H^1_f(F_v, V) = H^1_{ur}(F_v, V)$ (but assume $H^i(F_v, V) = 0$)

$v|p$ - $H^1_f(F_v, V) =$ classes of crystalline extensions

Bloch-Kato exponential map

$$DR(V_v)/F^0 \xrightarrow{\sim} H^1_f(F_v, V)$$

$$H^1_f(F, V) = \{x \in H^1(F, V)\ ,\ x_v \in H_f \text{ all } v\}$$

# Auxiliary data for the height pairing

- $\chi = \sum \chi_v : I_F/F^\times \to \mathbb{Q}_p$ - Idele class character.
- A choice, for each $v|p$ of a complementary subspace $W_v$ to $F^0$ in $DR(V_v)$.

E.g, for a curve $X$ complementary subspaces $W_v$ to $F^1$ in $H^1_{\mathrm{dR}}(X_v/F_v)$.

# Construction using mixed extensions

Assume having 2 maps

$$A \to H^1_f(F, V), \quad B^* \to H^1_f(F, V^*(1))$$

corresponding to extensions

$$0 \to V \to \mathcal{E}_1 \to A \to 0$$
$$0 \to B(1) \to \mathcal{E}_2 \to V \to 0$$

with $A$, $B$ trivial $G$ representations.

## Definition

A mixed extension of $\mathcal{E}_1$ and $\mathcal{E}_2$ is a representation $\mathcal{E}$ with a filtration $0 = W_{-3} \subset W_{-2} \subset W_{-1} \subset W_0 = \mathcal{E}$ and isomorphisms $W_{-1} \xrightarrow{\sim} \mathcal{E}_2$ and $\mathcal{E}/W_{-2} \xrightarrow{\sim} \mathcal{E}_1$

We get

$$0 \to \mathcal{E}_2 \to \mathcal{E} \to A \to 0$$
$$0 \to B(1) \to \mathcal{E} \to \mathcal{E}_1 \to 0$$

This data will give a decomposable height pairing

$$h([\mathcal{E}_1], [\mathcal{E}_2]) = \sum_v h_v([\mathcal{E}_1], [\mathcal{E}_2]) \in \mathrm{Hom}(A, B)$$

For $v \nmid p$

$$A \xrightarrow{[\mathcal{E}]} H^1(F_v, \mathcal{E}_2) \cong B \otimes H^1(F_v, \mathbb{Q}_p(1))$$

and use

$$H^1(F_v, \mathbb{Q}_p(1)) \cong F_v^\times \otimes \mathbb{Q}_p \xrightarrow{\chi_v} \mathbb{Q}_p$$

to get $h_v([\mathcal{E}_1], [\mathcal{E}_2]) \in \mathrm{Hom}(A, B)$

For $v|p$ do the same starting from $A \xrightarrow{[\mathcal{E}]} H^1_f(F_v, \mathcal{E}_2)$

But now we have to split

$$0 \to B \otimes H^1_f(F_v, \mathbb{Q}_p(1)) \to H^1_f(F_v, \mathcal{E}_2) \to H^1_f(F_v, V) \to 0$$

Equivalently, via Bloch Kato, split

$$0 \to B \to DR((\mathcal{E}_2)_v)/F^0 \to DR(V_v)/F^0 \to 0$$

which you do via

$$DR(V_v)/F^0 \xrightarrow{W_v} DR(V_v) \xrightarrow{Frob} DR((\mathcal{E}_2)_v) \to DR((\mathcal{E}_2)_v)/F^0$$

where *Frob* means Frobenius equivariant.

# The geometric situation

- $X/F$ a smooth complete curve, good reduction for all $v|p$.
- $V = H^1_{\text{ét}}(\bar{X}, \mathbb{Q}_p(1))$
- $\chi, W_v$ auxiliary data as above.
- $D, E \in \text{Div}_0(X)$ with disjoint supports

Compute $h(D, E)$ with the mixed extension

$$\mathcal{E}_1 = H^1_{\text{ét}}(\bar{X} - \overline{\text{Supp}\, D}, \mathbb{Q}_p(1)), \quad \mathcal{E}_2 = H^1_{\text{ét}}(\bar{X}; \overline{\text{Supp}\, E}, \mathbb{Q}_p(1)),$$
$$\mathcal{E} = H^1_{\text{ét}}(\bar{X} - \overline{\text{Supp}\, D}; \overline{\text{Supp}\, E}, \mathbb{Q}_p(1)) \ ,$$

- $v \nmid p$ - Obtained by intersection theory
- $v|p$ Same as Coleman-Gross height pairing (B 2004), also (B 2017) in the semi-stable reduction case.

# Local height $h_v$ for $v$ not dividing $p$

- $\tilde{X}_v$ regular model for $X_v$
- $\tilde{D}, \tilde{E}$ extensions of $D$ and $E$ to rational divisors on $\tilde{X}_v$, one of which has zero intersection with special fiber.

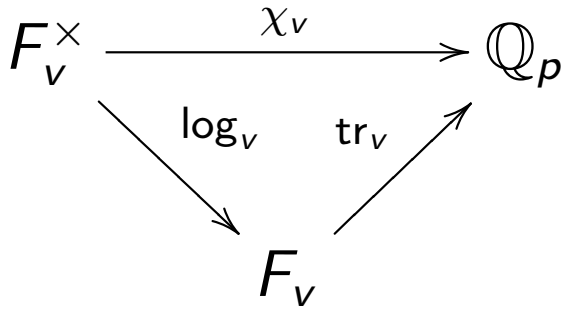
$$h_v(D, E) = \tilde{D} \cdot \tilde{E} \cdot \chi_v(\pi_v)$$

Key property - $h_v((f), E) = \chi_v(f(E))$ for a rational function $f$ (also when $v|p$) $\Rightarrow$ $h$ factors via $J$.

# The Coleman-Gross local height pairing $h_v$ (1989)

To compute $h_v(D, E)$ for $D, E \in \mathrm{Div}_0(X_v)$, $v|p$, with disjoint supports we need 2 ingredients

- A projection $\Psi : \Omega^1(X_v, \log(\mathrm{Supp}\, D)) \to H^1_{\mathrm{dR}}(X_v/F_v)$.
- Coleman integration theory (w.r.t. a fixed branch of the $p$-adic logarithm given by $\chi_v$).



# The Coleman-Gross local height pairing $h_v$ (1989)

## Definition

The local height pairing is $h_v(D, E) = \mathrm{tr}_v(\int_E \omega_D)$ where $\omega_D \in \Omega^1(X_v, \log(\mathrm{Supp}\, D))$ is the unique differential with

- $\mathrm{Res}\, \omega_D = D$.
- $\Psi(\omega_D) \in W_v$.

Note: Extends to bad reduction at $p$ using Vologodsky integration

# Heights for non-disjoint supports

- Gross, based on ideas of Tate
- Additional choice: Tangent vectors $\{t_P\ ,\ P \in X\}$.
- Local pairings should now satisfy
  - $h_v((f), E) = \chi_v(f[E])$ where $f[E]$ is a normalized value.
  - Change of vector formula: $t_P \to \alpha t_P$ adds $\chi_v(\alpha)\deg_P(D)\deg_P(E)$
- Formulas when $v$ does not divide $p$: Same, with $\tilde{P} \cdot \tilde{P} = 0$ provided $t_P$ is a generator of tangent bundle at $\tilde{P}$.
- Formulas when $v|p$: same with normalized values of integral.

# Decomposition of the height

Pick a differential $\omega$ on $X$ and use the dual tangent vector at (almost) every point.

$$h((P)-(P_0),(P)-(P_0)) = \sum_v h_v((P)-(P_0),(P)-(P_0))$$

**Theorem (B+Balakrishnan)**

*For an elliptic curve $E/\mathbb{Q}$ pick $\omega$ to be the invariant differential. Then*

$$h_p((P)-(\infty),(P)-(\infty)) = -2\tau(P), \quad (\tau = \int(\omega \times \int \bar{\omega}))$$

# Quadratic Chabauty for an elliptic curves $E/\mathbb{Q}$

Assume rank $E = 1$ and that $\int \omega$ does not vanish on $E(\mathbb{Q})$. Then, on $E(\mathbb{Q})$,

$$h((P)-(\infty),(P)-(\infty)) = \beta(\int_{\infty}^{P} \omega)^2 \text{ for some} \beta.$$

For an integral $P$ $LHS = \sum_q h_q((P)-(\infty),(P)-(\infty))$

- $h_p((P)-(\infty),(P)-(\infty)) = -2\tau(P)$
- $h_q((P)-(\infty),(P)-(\infty)) = 0$ when $E$ has good reduction at $q$
- $h_q((P)-(\infty),(P)-(\infty)) = 0$ can have a finite number of values when $E$ has bad reduction at $q$.

$\Rightarrow -2\tau(P) - \beta(\int_{\infty}^{P} \omega)^2 \in$ a finite computable set of values $T$.

# Quadratic Chabauty for a hyperelliptic curve

$X : y^2 + R(x)y = Q(x)$, $\deg Q = 2g + 1$

$$\omega_0 = \frac{dx}{2y + R(x)} \, , \omega_i = x^i \omega_0, i = 1, \ldots, g-1$$

standard dual basis $\bar{\omega}_i = (2i+1)x^{2g-1-i}\omega_0$

$$\tau = \sum_{i=0}^{g-1} \int (\omega_i \times \int \bar{\omega}_i)$$

**Theorem (B+Balakrishnan+Müller)**

*Appropriate choice* $\Rightarrow h_p((P) - (\infty), (P) - (\infty)) = -2\tau(P)$

# Quadratic Chabauty for a hyperelliptic curve

**Theorem (B. + Balakrishnan+ Müller)**

*Let $X$ be a hyperelliptic curve of genus $g$ in minimal model. Suppose that Chabauty's method does not apply to $X$ and that* $\mathrm{rank}(J) = g$. *Then there exists constants $a_{ij} \in \mathbb{Q}_p$ and a finite set of values $T$ such that*

$$I(P) = \sum_{i=0}^{g-1} \int (\omega_i \times \int \bar{\omega}_i) + \sum_{ij} a_{ij} (\int_\infty^P \omega_i)(\int_\infty^P \omega_j)$$

*obtains on each integral point of $C$ a value in $T$.*

# Proof

- Either Chabauty's method applies, or the functionals $\psi_i = \int \omega_i$ form a basis to $\mathrm{Hom}(J(\mathbb{Q}), \mathbb{Q}_p)$.
- $\psi_i \cdot \psi_j$ form a basis to the vector space of $\mathbb{Q}_p$ valued quadratic forms on $J(\mathbb{Q})$.
- $h$ is also quadratic, so we have $a_{ij}$ with $h + \sum a_{ij}\psi_i \cdot \psi_j = 0$
- Rest of the proof as for elliptic curves

# Number fields (B+Balakrishnan + Müller)

The above techniques can be applied to curves over number fields as well

- We look at $\mathbb{Q}_p$ points of restriction of scalars of $X$ to $\mathbb{Q}$, so need more equations.
- Some equations are provided by linear Chabauty (Siksek)
- Can sometimes use different idele class characters for more equations.

# The Mordell-Weil Sieve

The problem: eliminating "false positives"

- When solving $I(P) \in T$, many solutions will be "false positive"
- A true solution is easily recognized: solves the equation
- A false solution does not solve the equation in reasonably sized integers
- How to *prove* it is really false?

# The Mordell-Weil Sieve

The Mordell-Weil Sieve (Flynn, Bruin, Stoll, Elkies, Poonen) is a standard technique for proving non-existence of solutions, adapted to the problem.

Suppose $P \in X(\mathbb{Q}_p)$ is in $X(\mathbb{Q})$.

- We know $(P) - (P_0) = x \in J(\mathbb{Q})/p^k J(\mathbb{Q})$ for any $k$.
- Pick an auxiliary prime $l$ s.t. $p | \#J(\mathbb{Z}/l)$
- Then $P \pmod{l} \in X(\mathbb{Z}/l) \cap \left(x \pmod{l} + p^k J(\mathbb{Z}/l)\right)$.
- If this last set is empty we get a contradiction!