The Mordell–Weil Theorem and Canonical Heights

Michał Mrugała

ENS Lyon

December 2, 2025

Mordell–Weil Theorem

Theorem (Weak Mordell–Weil)

Let $n \in \mathbb{Z}_{>0}$, then $A(K)/nA(K)$ is finite.

$$\Big\downarrow \text{ descent via heights}$$

Theorem (Strong Mordell–Weil)

$A(K)$ is a finitely generated abelian group.

Proof Idea

Wish 1

We have a (semi)norm $\|\cdot\|$ on $A(K)$.

Claim

$A(K)$ is generated by $\{x \in A(K) : \|x\| \leq B\}$ for some B.

Wish 2

The set $\{x \in A(K) : \|x\| \leq B\}$ is finite.

Proof of Claim: Descent!

1. Fix $n \geq 2$.
2. By Weak Mordell–Weil $A(K)/nA(K)$ is finite. So there is a ball of finite radius C intersecting all cosets.
3. Let $z \in A(K)$. We can write $z = nx + y$ with $\|y\| < C$.
4. Then $\|x\| = \frac{\|z-y\|}{n} \leq \frac{\|z\|+C}{2}$.
5. Fix $\varepsilon > 0$.
6. When $\|z\| \gg C$ we have $C < \|z\| - \varepsilon$ and $\|x\| < \|z\| - \varepsilon$.
7. Hence B exists by descent!

Enter Heights

Let $\mathcal{L}$ be a line bundle on A and $h_{\mathcal{L}}$ be the associated height.

1. If $\mathcal{L}$ is ample, the set $\{x \in A(K) : h_{\mathcal{L}}(x) \leq B\}$ is finite for all B.
2. If $A = E$ is an elliptic curve, $\mathcal{L}$ corresponds to a multiple of (0) and $d \in \mathbb{Z}$ then $h_{\mathcal{L}}$ is a quadratic form up to $O(1)$.
3. If $\mathcal{L}$ is generated by its global sections then $h_{\mathcal{L}} \geq 0$ up to $O(1)$.
4. We only dealt with $h_{\mathcal{L}}$ up to $O(1)$.

Question 1

Is there a height $h_{\mathcal{L}} + O(1)$ which is a positive semidefinite quadratic form up to $O(1)$?

Question 2

Is there a representative $\widetilde{h}_{\mathcal{L}}$ of $h_{\mathcal{L}} + O(1)$ which is a bona fide positive semidefinite quadratic form?

Approximating a quadratic form

If $h_{\mathcal{L}}$ is a quadratic form it certainly has to satisfy

1. $h_{\mathcal{L}}(dx) = d^2 h_{\mathcal{L}}(x) + O(1)$,
2. $h_{\mathcal{L}}(x+y) + h_{\mathcal{L}}(x-y) = 2h_{\mathcal{L}}(x) + 2h_{\mathcal{L}}(y) + O(1)$.

Recall that $h_{\mathcal{L}}$ is functorial and additive in $\mathcal{L}$ up to $O(1)$, so it suffices to show that

1. $\mathcal{L}^{\otimes d^2} = [d]^*\mathcal{L}$,
2. $(\mathrm{pr}_1 + \mathrm{pr}_2)^*\mathcal{L} \otimes (\mathrm{pr}_1 - \mathrm{pr}_2)^*\mathcal{L} = \mathrm{pr}_1^* \mathcal{L}^{\otimes 2} \otimes \mathrm{pr}_2^* \mathcal{L}^{\otimes 2}$.

To find such an $\mathcal{L}$ we have to recall some standard facts about line bundles on abelian varieties.

Theorem of the Cube

Theorem

Let X, Y, Z be varieties with X, Y complete.
Let x, y, z be k-points of X, Y, Z and $\mathcal{L}$ be a line bundle on $X \times Y \times Z$.
Suppose that the restriction of $\mathcal{L}$ to each of

$$\{x\} \times Y \times Z, X \times \{y\} \times Z, X \times Y \times \{z\}$$

is trivial, then so is $\mathcal{L}$.

Consequences

Corollary

Let X be an abelian variety, $\mathcal{L}$ be a line bundle on X. For any variety Y and $f, g, h : X \to Y$

$$(f+g+h)^*\mathcal{L} \simeq (f+g)^*\mathcal{L} \otimes (g+h)^*\mathcal{L} \otimes (h+f)^*\mathcal{L} \otimes f^*\mathcal{L}^\vee \otimes g^*\mathcal{L}^\vee \otimes h^*\mathcal{L}^\vee.$$

Corollary

$$[d]^*\mathcal{L} \simeq \mathcal{L}^{\otimes \frac{d(d+1)}{2}} \otimes (i^*\mathcal{L})^{\otimes \frac{d(d-1)}{2}}.$$

So we need $\mathcal{L}$ to at least be ample and symmetric. In fact, by the Theorem of the Cube:

Corollary

If $\mathcal{L}$ is ample and symmetric, then $h_{\mathcal{L}}$ is a positive semidefinite quadratic form up to $O(1)$.

Getting Rid of $O(1)$

Lemma. (Tate). *Let S be a set and $\pi : S \to S$ a map. Let f be a real-valued function on S such that $f \circ \pi = \lambda f + O(1)$, with $\lambda > 1$. Then there is a unique function $\tilde{f}$ on S such that*

(a) $\tilde{f} = f + O(1)$
(b) $\tilde{f} \circ \pi = \lambda \tilde{f}$

and we have

$$\tilde{f}(x) = \lim_{n \to \infty} (1/\lambda^n) f(\pi^n x), \text{for every } x \in S.$$

Theorem. (Néron-Tate). *Let A be an abelian variety over $\bar{K}$. There is a unique function $c \mapsto \tilde{h}_c$ on $\mathrm{Pic}(A)$ with values in the space of real valued functions on $A(\bar{K})$ such that,*

1) $\tilde{h}_c(x) = h_c(x) + O(1)$.
2) *Additivity:* $\tilde{h}_{c_1+c_2} = \tilde{h}_{c_1} + \tilde{h}_{c_2}$.
3) *Functoriality: for all endomorphisms $\phi : A \to A$, we have*

$$\tilde{h}_{\phi^* c} = \tilde{h}_c \circ \phi \quad \text{for} \quad c \in \mathrm{Pic}(A).$$

Further if B is another abelian variety and $\psi : B \to A$ is a homomorphism, then

$$\tilde{h}_{\psi^* c} = \tilde{h}_c \circ \psi \quad \text{for all } c \in \mathrm{Pic}(A).$$

Properties of heights

From the theorem of the cube we see that if $\mathcal{L}$ is antisymmetric $\widetilde{h}_{\mathcal{L}}$ is linear.

Theorem 4.3. *Let $A/\bar{\mathbb{Q}}$ be an abelian variety, and let $\mathscr{L}$ be an invertible sheaf on A.*

(a) *There is a unique function*

$$\hat{h}_{\mathscr{L}}: A \to \mathbb{R}$$

with the following properties:

(i) *$\hat{h}_{\mathscr{L}}$ is a quadratic function (i.e. the map*

$$\langle\ ,\ \rangle: A \times A \to \mathbb{R},$$

$$\langle P, Q\rangle = \hat{h}_{\mathscr{L}}(P+Q) - \hat{h}_{\mathscr{L}}(P) - \hat{h}_{\mathscr{L}}(Q)$$

is bilinear.)

(ii) *$\hat{h}_{\mathscr{L}} = h_{\mathscr{L}} + O(1)$ on A.*

(b) *Assume now that $\mathscr{L}$ is ample and symmetric. Then*

(i) *$\hat{h}_{\mathscr{L}}(P) \geq 0$ for all $P \in A$.*

(ii) *$\hat{h}_{\mathscr{L}}(P) = 0$ if and only if P is a point of finite order.*

(iii) *More generally, $\hat{h}_{\mathscr{L}}$ is a positive definite quadratic form on $A(\bar{\mathbb{Q}}) \otimes \mathbb{R}$.*

Non-degeneracy

We will prove a slightly more general version:

Theorem. *Suppose that A is defined over $\bar{\mathbf{Q}}$. If c is ample, the quadratic part of $\tilde{h}_c$ is a positive non-degenerate form on $V = A(\bar{\mathbf{Q}})/A(\bar{\mathbf{Q}})_{\mathrm{tors}}$.*

Recall that a quadratic form on V is non-degenerate iff for all finite dimensional subspaces $V' \leq V$ the form is non-degenerate on $V' \otimes \mathbb{R}$.
WLOG, $\mathcal{L}$ is symmetric and $V' = A(K) \otimes \mathbb{Q}$.
By Northcott's Theorem, the set $\{x \in A(K) \otimes \mathbb{Q} : \widetilde{h}_{\mathcal{L}}(x) \leq B\}$ is finite for all B.

1. Let $V' \otimes \mathbb{R} \simeq \mathbb{R}^n$ such that $V' \simeq \mathbb{Z}^n$. If $\widetilde{h}_{\mathcal{L}}$ is degenerate, it comes from a projection $\pi : \mathbb{R}^n \to \mathbb{R}^{n-1}$. By Northcott the restriction $\pi|_{\mathbb{Z}^n}$ is injective.
2. By (1), $\pi(\mathbb{Z}^n)$ is not discrete, so there is a sequence of points $v_i \in \mathbb{Z}^n$ such that $\widetilde{h}_{\mathcal{L}}(v_i) \to 0$, contradicting Northcott.

Proof of Weak Mordell–Weil

Since to deduce Strong Mordell-Weil it suffices to prove Weak Mordell–Weil for some n and K I will assume that $A[n](K) = A[n](\overline{K})$.

1. For $a \in A(K)$ choose $b \in A(\overline{K})$ such that $nb = a$.
   For $\sigma \in G = \mathrm{Gal}(\overline{K}/K)$ define $\varphi_a(\sigma) = \sigma b - b$.
   This defines an injection $\Phi : A(K)/nA(K) \hookrightarrow \mathrm{Hom}(G, A[n](K))$.
2. There is an open subset $\mathrm{Spec}(R) \subset \mathrm{Spec}(\mathcal{O}_K)$ such that A extends to an abelian scheme $\mathcal{A}$ over $\mathrm{Spec}(R)$ and n is invertible in R.
3. For $a \in A(K)$, the normalization of R in $K(n^{-1}a)$ is étale over R.
   Hence $K(n^{-1}a)$ is unramified over R.
4. Each φ_a factor through an abelian extension of exponent n, unramified over R.
5. The maximal abelian extension K' of exponent n, unramified over R is finite over K. Then Φ factors through $\mathrm{Hom}(\mathrm{Gal}(K'/K), A[n](K))$.

A Cultural Remark

We have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow A[n](\overline{K}) \longrightarrow A(\overline{K}) \xrightarrow{\times n} A(\overline{K}) \longrightarrow 0.$$

Blackboard computations in progress...

Which results in the **fundamental exact sequence**

$$0 \to A(K)/nA(K) \to \mathrm{Sel}^m(A;k) \to Ш(A;k)[m] \to 0$$

Which results in the **fundamental exact sequence**

$$0 \to \underset{\substack{\uparrow \\ ???}}{A(K)/nA(K)} \longrightarrow \underset{\substack{\uparrow \\ \text{finite and computable}}}{\mathrm{Sel}^m(A;k)} \longrightarrow \underset{\substack{\uparrow \\ ???}}{Ш(A;k)[m]} \to 0$$