MA 254 notes: Diophantine Geometry
(Distilled from [Hindry-Silverman], [Manin], [Serre])

Dan Abramovich
Brown University
January 27, 2016
The Mordell-Weil theorem

Mordell Weil and Weak Mordell-Weil

Theorem (The Mordell-Weil theorem)

Let $A/k$ be an abelian variety over a number field. Then $A(k)$ is finitely generated.

We deduce this from

Theorem (The weak Mordell-Weil theorem)

Let $A/k$ be as above and $m \geq 2$. Then $A(k)/mA(k)$ is finite.
The reduction comes from the following.

**Lemma (Infinite Descent Lemma)**

Let $G$ be an abelian group, $q : G \to \mathbb{R}$ a quadratic form. Assume

(i) for all $C \in \mathbb{R}$ the set $\{ x \in G | q(x) \leq C \}$ is finite, and

(ii) there is $m \geq 2$ such that $G/mG$ is finite.

Then $G$ is finitely generated. In fact if $\{g_i\}$ are representatives for $G/mG$ and $C_0 = \max\{q(g_i)\}$ then the finite set $S := \{ x \in G | q(x) \leq C_0 \}$ generates $G$.

Indeed the canonical Néron-Tate height $\hat{h}_D$ on $A(k)$ associated to an ample symmetric $D$ gives a quadratic form satisfying (i), and (ii) follows from Weak Mordell-Weil. The Mordell-Weil theorem follows.
Proof of the Infinite Descent Lemma for $m \geq 3$

- $q(x) \geq 0$ otherwise the elements $\{nx\}$ would violate (i).
- Write $|x| = \sqrt{q(x)}$, $c_0 = \max\{|g_i|\}$,

$$S_{\sqrt{m^k}c_0} = \{x \in G : |x| \leq \sqrt{m^k}c_0\}.$$ 

- Clearly $G = \bigcup S_{\sqrt{m^k}c_0}$, so enough to show $S_{\sqrt{m^k}c_0} \subset \langle S \rangle$ for all $k$.
- We use induction on $k \geq 0$. Clearly $S_{c_0} = S \subset \langle S \rangle$.
- Assume $S_{\sqrt{m^k}c_0} \subset \langle S \rangle$ and let $x \in S_{\sqrt{m^{k+1}}c_0} \setminus S_{\sqrt{m^k}c_0}$.
- $x \in g_i + mG$ for some $i$ so there is $x_1$ such that $m x_1 = x - g_i$. So

$$|x_1| = \frac{|x - g_i|}{m} \leq \frac{|x| + |g_i|}{m} \leq \frac{\sqrt{m^{k+1}} + 1}{m}c_0 \leq \sqrt{m^k}c_0$$

since $m \geq 3$. ♠
Proof of Weak Mordell-Weil - Finite Kernel Lemma

**Lemma (Finite Kernel Lemma)**

Fix a finite \( k' / k \). Then \( \text{Ker} \left( \frac{A(k)}{mA(k)} \rightarrow \frac{A(k')}{mA(k')} \right) \) is finite.

**Proof of lemma**

- Note this kernel is \( B_{k'/k} := \frac{(A(k) \cap mA(k'))}{mA(k)} \).
- Since for a further extension \( k'' / k' \) we have \( B_{k'/k} \subset B_{k''/k} \), we may replace \( k' \) by a further extension.
- In particular we may assume \( k' / k \) Galois, with Galois group \( G \). The lemma now follows from the following, since \( G \) and \( A_m(\bar{k}) \) are finite:

**Sublemma**

There is an injective function \( B_{k'/k} \rightarrow \text{Maps}(G, A_m(\bar{k})) \).
Proof of Weak Mordell-Weil - reduction - sublemma

Proof of sublemma

- For $x \in B_{k'/k}$ fix $y \in A(k')$ such that $[m]y$ represents $x$.
- Consider the function $f_x : G \to A(k')$ where $f(\sigma) = y^\sigma - y$.
- Note $[m]f_x(\sigma) = [m](y^\sigma - y) = [my]^\sigma - [m]y = x^\sigma - x = 0$.
- This defines $B_{k'/k} \to Maps(G, A_m(\bar{k}))$.
- We claim it is injective.
- Assume $f_x = f_x'$, and let $y, y'$ be the chosen points in $A(k')$.
- So $y'^\sigma - y' = y^\sigma - y$, hence $(y' - y)^\sigma = y' - y$ for all $\sigma$.
- So $y' - y \in A(k)$ and $[m](y' - y) \in mA(k)$.
- Hence $x - x' = 0$ in $B_{k'/k}$, as needed.
Theorem (Chevalley-Weil+Hermite for \([m]\))

Fix an abelian variety \(A/k\) and an integer \(m\). There is a finite extension \(k'/k\) such that if \(x \in A(k)\) then there is \(y \in A(k')\) such that \([m]y = x\).

Proof of Weak Mordell-Weil assuming Chevalley-Weil+Hermite

Let \(k'\) be as in Chevalley-Weil+Hermite for \([m]\). Then the map \(A(k)/mA(k) \to A(k')/mA(k')\) is zero, hence by the Finite Kernel Lemma \(A(k)/mA(k)\) is finite.

We will present two proofs of Chevalley-Weil+Hermite: one quick and dirty using Scheme Theory. One going through with rings and differentials explicitly.
Hermite’s theorem(s)

The following classical theorem appears in a first course:

Theorem (Hermite 1)

For any real $B$ there are only finitely many number fields $k$ with $|d_k| \leq B$.

This one might not be as visible:

Theorem (Hermite 2)

For any integer $n$ and finite set of primes $S$ there are only finitely many number fields $k$ unramified outside $S$ with $[k : \mathbb{Q}] \leq n$.

Hermite 2 follows from Hermite 1 given the following:

Proposition (Discriminant bound (Serre), not proven here)

Write $[k : \mathbb{Q}] = n$ and $N = \prod_{p|d_k} p$. Then $|d_k| \leq (N \cdot n)^n$. 
Why number-theorists want to understand schemes

What I stated as “Chevalley-Weil+Hermite” is a consequence of

**Proposition (Spreading out)**

Let \( \phi : Y \to X \) be a finite unramified morphism of projective varieties, all over \( k \). Then there is a finite set of primes \( S \), projective schemes \( \mathcal{X} \to \text{Spec} \mathcal{O}_{k, S} \), \( \mathcal{Y} \to \text{Spec} \mathcal{O}_{k, S} \) and a finite unramified morphism \( \varphi : \mathcal{Y} \to \mathcal{X} \), whose restriction to \( \text{Spec} k \) is \( \phi : Y \to X \).
Spreading out: Picture with point
The Mordell-Weil theorem

Spreading out implies Chevalley-Weil

The reduction works as follows:

- In our case take $X = Y = A$ and $\phi = [m]$.
- Since $\mathcal{X} \to \text{Spec} \mathcal{O}_{k,S}$ projective, a point $x \in X(k)$ extends to a morphism $\tilde{x} : \text{Spec} \mathcal{O}_{k,S} \to \mathcal{X}$.
- Write $\mathcal{Y}_x = \text{Spec} \mathcal{O}_{k,S} \times_{\mathcal{X}} \mathcal{Y}$.
- Since $\mathcal{Y} \to \mathcal{X}$ is unramified we have $\Omega_{\mathcal{Y}/\mathcal{X}} = 0$.
- $\Omega_{\mathcal{Y}_x/\text{Spec} \mathcal{O}_{k,S}}$ is the pullback of this to $\mathcal{Y}_x$, so also 0.
- If $[m]y = x$ then $y \subset \mathcal{Y}_x$ and its closure $\tilde{y}$ is unramified over $\tilde{x}$.
- This means that $\mathcal{O}(\tilde{y})$ is finite unramified over $\mathcal{O}_{k,S}$, so $k(y)/k$ unramified away from $S$.
- By Hermite 2 there are only finitely many such $k(S)$. Let $k'$ be the Galois closure of their compositum.
- so $y \in A(k')$. ♠
Step 1: Coordinates

- Say $Y \in \mathbb{P}^m$ and $X \in \mathbb{P}^n$. We may replace $Y \subset \mathbb{P}^m$ by the graph of $\phi$.
- We now have $Y \subset \mathbb{P}^m \times \mathbb{P}^n$, and $\phi$ is the restriction of the natural projection $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$.
- For each coordinate $X_i$ of $\mathbb{P}^n$ we have $U_i = X \setminus Z(X_i)$ affine, with coordinate ring $A_i = k[x_0, \ldots, x_i, \ldots, x_n]/(f_{1i}, \ldots, f_{ri})$.
- “$\phi$ finite” means: preimage of affine is affine, corresponding to a finite ring extension.
- So $V_i = \phi^{-1}U_i$ affine, with ring $B_i$ finite over $A_i$. Let $\{y_{1i}, \ldots, y_{ki}\}$ be module generators and $g_{ji}$ the module relations and $Y_{ji}Y_{j'i} = h_{jj'i}$ the ring relations, with $g_{ji}$, $h_{jj'i}$ $A_i$-linear in $Y_{1i}, \ldots, Y_{ki}$:

$$B_i = A_i[Y_{1i}, \ldots, Y_{ki}]/\langle \{g_{ji}\}, \{Y_{ji}Y_{j'i} - h_{jj'i}\} \rangle.$$
**Step 2: Shrinking to Define Rings and Maintain Finiteness**

- There are finitely many nonzero coefficients \( \{a_\alpha\} \) in \( f_{j,i}, g_{ji}, h_{jj',i} \), giving a subring \( \mathcal{O}_{k,S_0} := \mathcal{O}_k[\{a_\alpha, a_\alpha^{-1}\}] \) of \( k \) in which \( a_\alpha \) are units. Here \( S_0 \) is the set of places appearing in the factorizations of the \( a_\alpha \).

- Let \( A_i = \mathcal{O}_{k,S}[x_0, \ldots, x_{r_i}]/(f_{1,i}, \ldots, f_{r_i,i}) \) and \( B_i = A_i[Y_{1,i}, \ldots, Y_{k,i}]/(\{g_{ji}\}, \{Y_{ji} Y_{j',i} - h_{jj',i}\}) \).

- We clearly have \( A_i = A_i \otimes_{\mathcal{O}_{k,S}} k \) and \( B_i = B_i \otimes_{\mathcal{O}_{k,S}} k \).

- By construction \( A_i \langle Y_{ji} \rangle \to B_i \) is a surjective module homomorphism.

- So \( B_i \) is a finite \( A_i \)-algebra.
**Step 3: Shrinking to Evade Ramification**

- The statement "\( Y \to X \) unramified" is equivalent to "\( V_i \to U_i \) unramified".
- This is equivalent to "\( \Omega_{B_i/A_i} = 0 \)".
- Consider the finitely generated \( B_i \)-module \( \Omega_{B_i/A_i} \).
- We have \( \Omega_{B_i/A_i} \otimes_{O_{k,S}} k = \Omega_{B_i/A_i} = 0 \).
- So \( \text{Ann}_{O_{k,S}}(\Omega_{B_i/A_i}) \neq 0 \). In other words there is nonzero \( c \in O_{k,S} \) such that \( c\Omega_{B_i/A_i} = 0 \).
- Replacing \( O_{k,S} \) by \( O_{k,S}[c^{-1}] \subset k \) we may assume \( \Omega_{B_i/A_i} = 0 \), hence \( B_i \) is an unramified \( A_i \)-algebra.

In the language of spreading out, \( \mathcal{Y} := \cup \operatorname{Spec} B_i \) and \( \mathcal{X} := \cup \operatorname{Spec} A_i \).  

\( \blackspade \) (Spreading Out)
Proposition

Let $x \in X(k)$ and $\phi(y) = x$. Then $k(y)/k$ is unramified outside $S$.

- Fix a nonzero prime $p \subset \mathcal{O}_{k,S}$. We show $k(y)/k$ is unramified at $p$.
- Let $x = (\alpha_0, \ldots, \alpha_n) \in X$. Since $\mathcal{O}_{k,p}$ is principal we can take $\alpha_i \in \mathcal{O}_{k,p}$ relatively prime.
- Without loss of generality the uniformizer $\pi_p \not| \alpha_0$.
- Replacing $\alpha_i$ by $\alpha_i/\alpha_0$ we may assume $\alpha_0 = 1$.
- Consider the epimorphism $A_0 \rightarrow k$ given by the maximal ideal $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$.
- It gives $(A_0)_p \xrightarrow{\tilde{x}} \mathcal{O}_{k,p}$ (the image is no bigger).
Proof of the proposition

- Consider $\mathcal{C} := B_0 \otimes_{A_0} \mathcal{O}_{k,p}$.
- Since $A_0 \to B_0$ is finite and unramified, also $\mathcal{O}_{k,s} \to \mathcal{C}$ is finite and unramified.
- Consider the commutative diagram

\[
\begin{array}{ccccccccc}
B_0 & \longrightarrow & C & \dashrightarrow & & & & & \\
\uparrow & & \uparrow & & & & & & \\
A_0 & \longrightarrow & \mathcal{O}_{k,p} & \longrightarrow & B_0 & \longrightarrow & k(y) & & \\
& & \downarrow & & \downarrow & & \downarrow & & \\
& & A_0 & \longrightarrow & k & & & & \\
\end{array}
\]

- The universal property of tensor gives an arrow $\mathcal{C} \to k(y)$.
- Its image is a subring $R_{y,p} \subset k(y)$ finite unramified over $\mathcal{O}_{k,p}$, which must be $\mathcal{O}_{k(y),p}$.