DIOPHANTINE GEOMETRY WEEKS 09-10

XIAORUN WU

Abstract. For the next two weeks, we extend the results of [11], and will present proof of the Mordell-Weil Theorem for general Abelian Varieties. Again following the approach as outlined in [1], we now introduce additional tools that allows us to complete the proof of general Mordell-Weil Theorem for Abelian Varieties.

Contents

1. Introduction

The main objective of these two weeks is to extend the result on strong Mordell-Weil theorem for Elliptic Curves to Abelian Varieties, namely the finite generation of the group of rational points of an Abelian variety defined over a number field.

We already see in week 08 for a historical overview. Now we will introduce some additional tools that would allow us to extend this result to general Mordell-Weil Theorem.

As in the case of Elliptic Curve, we will split into two steps: in the first step, we will outline the proof for weak Mordell-Weil Theorem for general abelian varieties, then we give a generalized version of Fermat's descent theorem, which will allow us to prove strong Mordell-Weil Theorem.

2. The Weak Mordell-Weil Theorem for Abelian Varieties

The first step of proving Mordel-Weil for Abelian Varieties is to prove the Weak Mordel-Weil Theorem:

Theorem 2.1 (Weak Mordell-Weil). *Let A be an abelian variety over a number field K and let m be a positive integer. Then $A(K)/mA(K)$ is finite.*

To prove this, we need a few tools, among which the most important ones are Galois cohomology and Kummer theory. But before that, let us recall the definition of Abelian Varieties, and some of the useful lemmas we proved in [11], which will be useful in proving the Weak Mordell-Weil.

Definition 2.2 (Group Variety). *A variety G with morphisms*

$$m : G \times G \to G, (x, y) \mapsto xy\,(multiplication),$$
$$\iota : G \to G, x \mapsto x^{-1}\,(inverse),$$

and with an element $\epsilon \in G(K)$ is called a group variety (over K) if $G(\overline{K})$ is a group with multiplication, inverse, identity induced by m, ι, ε.

An **abelian variety** is a group variety that is either irreducible or reducible but geometrically complete.

The first step is to prove Mordell-Weil Theorem for Abelian Varieties. Recall that in the proof of weak Mordell-Weil Theorem for elliptic curves, we presented the following lemma:

Lemma 2.3. *Let A be an abelian variety defined over a field K and let L be a finite separable extension of K. Let m be a positive integer and suppose that $A(L)/mA(L)$ is a finite group. Then $A(K)/mA(K)$ is a finite group.*

We also state the following powerful result, which guarantees the existence of a number field upon unramified finite morphism. First we define local discriminant as:

Definition 2.4 (local discriminant). *Let $\varphi : Y \to X$ be a morphism of K-varieties and let $P \in Y(K)$ with image $Q \in X(K)$. Since φ is defined over K, we have $K(Q) \subset K(P)$ and $R_Q = K(Q) \cap R_P$. We then define the local discriminant as*

$$\widehat{\mathfrak{d}}_{P/Q} := \{\det(Tr_{\widehat{K(P)}/\widehat{K(Q)}}(a_ib_j))|a_1, \cdots, a_{\widehat{d}}, b_1, \cdots, b_{\widehat{d}} \in \widehat{R}_P\},$$

where $\widehat{d}$ is short for the local degree $\widehat{d}_P := [\widehat{K(P)}/\widehat{K(Q)}]$.

With this, the global Chevalley–Weil theorem has the following form:

Theorem 2.5. *Assume that $\varphi : Y \to X$ is a finite unramified morphism of K-varieties and that $(E^u)_{u\in M}$ is an M-bounded family in X. Then for any $v \in M_K$, there is a non-zero $\alpha_v \in R_v$ such that $\alpha_v \in \widehat{\mathfrak{d}}^u_{P/Q}$ whenever $u \in M$ with $u|v$ and $P \in Y(K)$ with $Q := \varphi(P) \in E^u$. Moreover, we can choose $\alpha_v = 1$ for all but finitely many $v \in M_K$.*

Specifically to number fields, we have:

Theorem 2.6 (Chevalley–Weil, number fields). *Let K be a number field and let $\varphi : Y \mapsto X$ be an unramified finite morphism of K-varieties. If X is complete, then there is a non-zero $\alpha \in O_K$ such that for any $P \in Y(\overline{K})$ and $Q := \varphi(P)$ the discriminant $\mathfrak{d}_{P/Q}$ of $O_{K(P)}$ over $O_{K(Q)}$ contains α.*

With this, we now switch gear and get a closer look to Galois Cohomology.

3. Galois Cohomology & Kummer Theorem: a brief taste

We denote $\mathrm{Gal}(L/K)$ the Galois group of an intermediate field extension $K \subset L \subset \overline{K}$. Let $g \in \mathrm{Gal}(L/K)$ and let X be a variety over K. Embed points $x \in X(L)$ into some affine chart, with affine coordinates in L. Applying g^{-1} to the coordinates, we get a well-defined point $x^g \in X(L)$. Clearly, $x^{gh} = (x^g)^h$ and hence we have an action of the Galois group on $X(L)$. If $\varphi : X \to Y$ is a morphism over K, then $\varphi(x^g) = \varphi(x)^g$. If F denotes the fixed field of $\mathrm{Gal}(L/K)$, then $x \in X(F)$ is equivalent to $x^g = x$ for every $g \in \mathrm{Gal}(L/K)$.

In particular, if X is an abelian variety A, we have $(ma)^g = ma^g$ and $(a+b)^g = a^g + b^g$ for $a, b \in A(L)$ and $m \in \mathbb{Z}$. Also recall that $A[m]$ denotes the group of m-torsion points of A.

With this, we have the following lemma:

Lemma 3.1. *Let L be a finite Galois extension of K and let $m \in \mathbb{Z} \setminus \{0\}$. If $A(L)/mA(L)$ is finite, then $A(K)/mA(K)$ is finite.*

Proof. The inclusion $A(K) \subset A(L)$ induces a homomorphism

$$A(K)/mA(K) \to A(L)/mA(L)$$

of abelian groups. Let N be its kernel. It suffices to show that N is finite. Choose a system of representatives in $A(K)$ for N. For each representative a, choose $b_a \in A(L)$ such that $a = mb_a$. Consider an element $g \in \mathrm{Gal}(L/K)$ and define

$$\lambda_a(g) := b_a^g - b_a.$$

Now by obseration above we have

$$m\lambda_a(g) = (mb_a)g - mb_a = ag - a.$$

By K-rationality of a, this is zero. Using our system of representatives, the rule $a \mapsto \lambda_a$ defines a map from N to the set of maps

$$\mathrm{Gal}(L/K) \to A[m].$$

N will be finite if the map is injective and the range is finite. The latter statement follows from Proposition 5.1 of [11]. In order to prove the former, let us suppose that $\lambda_a = \lambda_{a'}$ for representatives a, a'. We have

$$b_{a'}^g - b_{a'} = b_a^g - b_a$$

and hence

$$(b_{a'} - b_a)^g = b_{a'} - b_a$$

for every g, or equivalently $b_{a'} - b_a \in A(K)$. Therefore, by applying $[m]$ we get $a = a'$. $\square$

We next introduce Kummer theory for Abelian Varieties, which would be a very important step in the generalization of Weak Mordell-Weil Theorem.

We first make the following observation: let $m \in \mathbb{Z} \setminus \{0\}$ be not divisible by $\mathrm{char}(K)$, and assume that $A[m] \subset A(K)$. We denote the separable algebraic closure of K in $\overline{K}$ by K^s. For $a \in A(K)$, there is $b \in A(K^s)$ such that $a = mb$ (using $[m]$ unramified from Proposition 5.1 of [11], every such $b \in A(\overline{K})$ is in $A(K^s)$). If $g \in \mathrm{Gal}(K^s/K)$, then we define

$$\langle a, g \rangle := b^g - b.$$

and from the obvervation at the beginning of the chapter, we have $\langle a, g \rangle \in A[m]$.

Let $a' \in A(K)$ and $b' \in A(K^s)$, with $a' = mb'$, then

$$(b + b')^g - (b + b') = (b^g - b) + (b'^g - b').$$

This shows that $\langle a, g \rangle$ is independent of the choice of b (choose $b' \in A[m]$ and use that $b' \in A(K)$ by assumption). Moreover, we see that $\langle , \rangle$ is linear in the first variable.

Owing to all those observations, we may make the following definition:

Definition 3.2 (Kummer Pairing)**.** *Given $a \in A(K)$ and $g \in \mathrm{Gal}(K^*/K)$, then we may define **Kummer Pairing** as*

$$\langle , \rangle : A(K) \times \mathrm{Gal}(K^s/K) \to A[m].$$

We further define the right kernel as

$$\{g \in \mathrm{Gal}(K^s/K) \mid \langle a, g\rangle = 0, \quad \forall a \in A(K)\},$$

and the left kernel as

$$\{a \in A(K) \mid \langle a, g\rangle = 0, \quad \forall a \in A(K)\},$$

Now we define let $K(\frac{1}{m}A(K))$ to be the smallest intermediate field $K \subset L \subset \overline{K}$ such that any $b \in A(K)$ with $mb \in A(K)$ is rational over L.

Proposition 3.1. *The Kummer pairing is bilinear, with left-kernel $mA(K)$ and right-kernel the subgroup $\mathrm{Gal}(K^s/K(\frac{1}{m}A(K))$ of $\mathrm{Gal}(K^s/K)$.*

Proof. Let $g, g' \in \mathrm{Gal}(K^s/K)$. Let $a \in A(K)$. Then we have

$$\langle a, gg'\rangle = b^{gg'} - b = (b^g - b)^{g'} + b^{g'} - b.$$

Since $\langle a, g\rangle$ is K-rational by assumption, we get

$$\langle a, gg'\rangle = \langle a, g\rangle + \langle a, g'\rangle.$$

This proves linearity in the second variable and thus $\langle , \rangle$ is bilinear. For $a \in mA(K)$, choose $b \in A(K)$ such that $a = mb$. By K-rationality of b, we have

$$\langle a, g\rangle = bg - b = 0$$

for every $g \in \mathrm{Gal}(K^s/K)$. Conversely, let a be in the left-kernel. For any $b \in A(K^s)$ with $a = mb$, we have

$$0 = \langle a, g\rangle = bg - b.$$

Since this is true for every $g \in \mathrm{Gal}(K^s/K)$ and since K is the fixed field of the Galois group, we conclude $b \in A(K)$. So the left-kernel is equal to $mA(K)$.

Finally, we note that $\mathrm{Gal}(K^s/K(\frac{1}{m}A(K))$ is contained in the right-kernel H. On the other hand, let g be an element of the right-kernel. For $b \in A(K^s)$ with $mb \in A(K)$, we have $b^g = b$. It follows that the restriction of g to the residue field $K(b)$ is equal to the identity, hence the same is true for the restriction of g to to $K(\frac{1}{m}A(K))$. This proves $H \subset \mathrm{Gal}(K^s/K(\frac{1}{m}A(K))$. We conclude that equality holds. □

With all these, we would be able to prove the weak Mordell-Weil Theorem for Abelian Varieties.

Proof. It follows from Proposition 3.1 that the right-kernel is a closed normal subgroup of $\mathrm{Gal}(K^s/K)$. By Galois theory, $K(\frac{1}{m}A(K))$ is a Galois extension of K. By the same Proposition , we conclude that the Kummer pairing induces a nondegenerate pairing

$$(A(K)/mA(K) \times \mathrm{Gal}\, K(\frac{1}{m}A(K))/K \to A[m]$$

(i.e. left- and right-kernel are zero). Thus in order to prove the finiteness of the group $A(K)/mA(K)$, it is enough to show that $\mathrm{Gal}(K(\frac{1}{m}A(K))/K)$ is finite.

But this is obvious: By Lemma 3.1 and Proposition 5.1 of [11], we may assume that $A[m] \subset A(K)$. Since here K is a number field, we see that $K(\frac{1}{m}A(K)/K)$ is finite by Chevalley-Weil Theorem for number fields. This concludes the proof of the weak Mordell–Weil theorem. □

Now we've completed our first steps towards the proof of Mordell-Weil Theorem. In the following chapter, we will give a basic flavor of Néron-Tate height, which we will be used to prove the Fermat's Descent Theorem, the second step towards completing the proof of Mordell-Weil Theorem for Abelian Varieties.

4. Néron Tate Height and Fermat's Descent Theorem

See week 7's notes. This is a repetition of materials there, included for coherence

So ultimately, our goal is to prove the following lemma, which will be crucial in completing the proof of Mordell-Weil Theorem:

Lemma 4.1. *Let K be a number field and let c be ample and even. Then $\widehat{h}_c$ vanishes exactly on the torsion subgroup of $A(K)$. Moreover, there is a unique scalar product $\langle , \rangle$ on the abelian group $A(K) \otimes_{\mathbb{Z}} \mathbb{R}$ such that*

$$\widehat{h}_c(x) = \langle x \otimes 1, x \otimes 1 \rangle$$

for every $x \in A(K)$,

where we will soon define $\widehat{h}$, which is commonly known as Néron-Tate Height. Over the rest of the section, we will give a survey of important results in Néron-Tate heights.

Let K be a field and let A be an abelian variety over K. Let X be a complete variety over K. Then we know that we have the height homomrphism

$$\mathbf{h} : \mathrm{Pic}(X) \to \mathbb{R}^{X(\overline{K})}/O(1),$$

which associates $\mathbf{c}$ with the equivalence class of heights $\mathbf{h_c}$.

But the problem with Weil Heights is, there do not exist a canonical height function associated to $\mathbf{c} \in \mathrm{Pic}(X)$, as they are only determined up to a bounded constant.

To solve this, we take our resolution to theorem of cube. for every $\mathbf{c} \in \mathrm{Pic}(A)$ we have a quadratic function

$$\mathrm{Mor}(X, A) \to \mathrm{Pic}(X), \quad \varphi^* \mapsto \varphi^*(c).$$

where we may decompose $\mathbf{c}$ into an even and odd part $\mathbf{c} = \mathbf{c}_+ + \mathbf{c}_-$, and we there fore have the associated decomposition of height homomorphism:

$$q : \mathrm{Mor}(X, A) \to \mathbb{R}^{X(\overline{K})}O(1), \quad \varphi \mapsto \mathbf{h}_{\varphi^*(c)}.$$

We conclude that $q = q_+ + q_-$ for the quadratic form $q_+(\varphi) := h_{\varphi *}(c_+)$ and the linear form $q_-(\varphi) := h_{\varphi *}(c_-)$. The most important fact is that, this decomposition is unique. Motivating by the observation, we have the following:

Observation 4.1. *Let $h_{\boldsymbol{c}\pm}$ be an arbitrary height function in the class $\boldsymbol{h}_{\boldsymbol{c}\pm}$. For any integer n, we have $n^2\boldsymbol{h}_{c_+} = \boldsymbol{h}_{[n]*(c_+)}$ and $n\boldsymbol{h}_{c_-} = \boldsymbol{h}_{[n]*(c_-)}$. By theorem of height function, there is a constant $C(n)$ such that for every $a \in A$*

$$|h_{c+}(na) - n^2 h_{c+}(a)| \leq C(n)$$

and

$$|h_{c-}(na) - n h_{c-}(a)| \leq C(n).$$

Definition 4.2 (Quasi-Homogeneous)**.** *Let $\mathcal{N}$ be a multiplicatively closed subset of $\mathbb{R}$ (resp. $\mathbb{R}_+$) acting on a set S by means of a map such that $n(mx) = (nm)x$ for $x \in S$. A function $h : S \to R$ is quasi-homogeneous of degree $d \in N$ (resp. $d \in R+$) for N if for $n \in \mathbb{N}$ there is a positive constant $C(n)$ such that*

$$|h(nx) - n^d h(x)| \leq C(n)$$

for every $x \in S$, and is homogeneous of degree d for N if $h(nx) = ndh(x)$.

We then have the following theorem:

Theorem 4.3. *Let $\mathcal{N}$ act on the set S as before and let $h : S \to \mathbb{R}$ be quasihomogeneous of degree $d > 0$. If $\mathcal{N}$ has an element of absolute value > 1, then there is a unique homogeneous function $\widehat{h} : S \to R$ of degree d for $\mathcal{N}$ such that $\widehat{h} - h$ is bounded.*

The proof of this is purely algebraic, which we will omit here. The readers are welcome to check [1], chapter 9.

We then introduce the Tate's limit argument:

Theorem 4.4. *Let $\boldsymbol{c} \in Pic(A)$ and let $\boldsymbol{c} = \boldsymbol{c}_+ + \boldsymbol{c}_-$ be a decomposition into an even part $\boldsymbol{c}+$ and an odd part $\boldsymbol{c}_-$. Then the classes $\boldsymbol{h}_{c_\pm}$ are independent of the choice of the decomposition. There is a unique homogeneous height function $\widehat{\boldsymbol{h}}_{c_\pm}$ in the class $\boldsymbol{h}_{c_\pm}$, of degree 2 in the $+$ case and degree 1 in the $-$ case.*

This theorem allows the definition of Néron-Tate height:

Definition 4.5 (Néron-Tate height)**.** *The height function $\widehat{\boldsymbol{h}}_c := \widehat{\boldsymbol{h}}_{c_+} + \widehat{\boldsymbol{h}}_{c_-}$ is called the Néron–Tate height associated to c.*

To complete this section, we associate our bilinear form with Néron Tate Height, which would allow us to prove the Fermat Descent Theorem.

Let M be an abelian group and let b be a real-valued symmetric bilinear form on M. We have in mind the example $M = A(K)$ and a certain bilinear form associated to a Néron–Tate height. The kernel of b is the abelian group

$$N := \{x \in M | b(x, y) = 0 \text{ for every } y \in M\}.$$

Then b induces a symmetric bilinear form b on $\overline{M} := M/N$ and the kernel of b is zero. Since b is real valued, $\overline{M}$ is torsion free and all torsion elements of M are contained in N. We conclude that

$$\overline{M} \to \overline{M}_{\mathbb{R}} := \overline{M} \otimes_{\mathbb{Z}} \mathbb{R}, mm \otimes 1$$

is injective. Let $\overline{M}'$ be a finitely generated subgroup of $\overline{M}$. The restriction of b to the free abelian group $\overline{M}'$ extends uniquely to a bilinear form $\overline{b}'$ on $\overline{M}'_{\mathbb{R}}$. Let $\overline{M}'_{\mathbb{Q}} = \overline{M}' \otimes_{\mathbb{Z}} \mathbb{Q}$. An easy argument shows that

$$\overline{M}'_{\mathbb{Q}} \subset \overline{M}_{\mathbb{Q}}$$

and so $\overline{M}'_{\mathbb{R}} \subset \overline{M}_{\mathbb{R}}$. Since $\overline{M}_{\mathbb{R}}$ is the union of all $\overline{M}'$ and the bilinear forms $\overline{b}'$ coincide on overlappings by uniqueness, we have a unique extension of b to a bilinear form $b_{\mathbb{R}}$ on $\overline{M}_{\mathbb{R}}$.

Thus we would like that bilinear form on $b_{\mathbb{R}}(x, y)$ determines a scalar product and an associated norm $\|x\|^2 = b_{\mathbb{R}}(x, x)$ on $M_{\mathbb{R}}$. In fact, we have the following lemma:

Lemma 4.6. *With the notation and assumptions above, the bilinear form $b_{\mathbb{R}}$ is positive definite if and only if for every finitely generated subgroup $\overline{M}'$ of $\overline{M}$ and for every $C > 0$ the set*

$$\{x \leq \overline{M} \mid b_{\mathbb{R}}(x,x) \leq C\}$$

is finite.

Finally, our goal is to offer a explicit formula that would allow us to calculate Néron-Tate heights.

Theorem 4.7. *Let K be a number field and let c be ample and even. Then $\widehat{h}_c$ vanishes exactly on the torsion subgroup of $A(K)$. Moreover, there is a unique scalar product $\langle , \rangle$ on the abelian group $A(K) \otimes_{\mathbb{Z}} \mathbb{R}$ such that*

$$\widehat{h}_c(x) = \langle x \otimes 1, x \otimes 1 \rangle$$

for every $x \in A(K)$.

For a complete proof of this would require more algebraic geometry input, which we shall omit here.

With this, we are now ready to prove the second part-Fermat Descent Theorem.

5. Putting it altogether

Recall that Mordell-Weil Theorem states the following:

Theorem 5.1 (Mordell-weil)**.** *If A is an abelian variety over a number field K, then $A(K)$ is a finitely generated abelian group.*

And the final missing piece is the following:

Theorem 5.2 (Fermat's Descent)**.** *Let G be an abelian group and let $m \geq 2$ be a positive integer. Let also $\| \ \|$ be a real function on G satisfying*

$$\|x - y\| \leq \|x\| + \|y\|, \ \ \|mx\| = m\|x\|$$

for any $x, y \in G$. Assume that S is a set of representatives for G/mG, bounded relative to $\| \ \|$ by a constant C. Then for any $x \in G$, there is a decomposition

$$x = \sum_{i=0}^{l} m^i y_i + m^{l+1} z,$$

where $y_i \in S$ and where $z \in G$ satisfies $\|z\| \leq C + 1$. In particular, G is generated by elements in the ball

$$\{x \in G \mid \|x\| \leq C + 1\}.$$

Proof. There are $y_0 \in S$, $x_0 \in G$ such that $x = y_0 + mx_0$. We have

$$\|x_0\| \leq \frac{1}{m}(C + \|x\|).$$

Proceeding by induction, there are $y_l \in S$, $x_l \in G$ such that $x_{l-1} = y_l + mx_l$ and

$$\|xl\| \leq \left(\sum_{i=1}^{l+1} \frac{1}{m^i} \right) \cdot C + \frac{1}{m^{l+1}} \|x\|.$$

We choose l so large that $\|x\| \leq m^{l+1}$ and set $z := x^l$, getting

$$\|z\| \leq \frac{1}{m-1} \cdot C + 1 \leq C + 1.$$

Moreover, we have

$$x = y_0 + my_1 + \cdots + m^l y_l + m^{l+1} z,$$

which proves the first claim. The second claim is a trivial consequence of the first. □

Now theorem 5.1 is just a direct consquence of 5.2 and 4.7.

Proof. Choose an integer $m \geq 2$. The weak Mordell–Weil theorem gives the finiteness of $A(K)/mA(K)$. By results about abelian variety (e.g. see 8.6.4 of [1]), there is an even ample $\mathbf{c} \in \mathrm{Pic}(A)$. By Theorem 4.7, the assumptions of Theorem 5.2 for $\|\cdot\| := \widehat{h}_{\mathbf{c}}^{1/2}$ on $G := A(K)$ are satisfied. Therefore 5.2 shows that the group $A(K)$ is generated by a bounded set. Finally, Northcott's theorem in [11] shows that $A(K)$ is finitely generated. □

With this we completed the proof of strong Mordell-Weil Theorem.

Acknowledgements

I would like to thank Prof. Yunqing Tang for her generous guidance and invaluable advice over the project, and I would also like to thank Shiji Lyu, whose help and suggestions had helped me pushed beyond boundaries. All those work would not be possible, of course, with the consistent support of my family and friends.

References

[1] Bombieri, Enrico, and Walter Gubler. 2006. *Heights in diophantine geometry.* Cambridge: Cambridge University Press. `http://public.eblib.com/choice/publicfullrecord.aspx?p=244411`

[2] Robin Hartshorne, *Algebraic Geometry* Graduate Texts in Mathematics, Vol. **52** Chapter 1, pp. 54, Springer Science & Business Media, 2013

[3] N. Jacobson, *Basic Algebra II.* First edition. W. H. Freeman & Co., San Francisco 1980. xix+666 pp. Second edition. W. H. Freeman & Company, New York 1989. xviii+686 pp.

[4] S. Lang, *Algebraic Number Theory.* Second edition. Graduate Texts in Mathematics 110. Springer-Verlag, New York 1994. xiv+357 pp.

[5] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.* Proc. Cambridge Philos. Soc. **21** (1922), 179–192.

[6] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* Second Edition. PWN– Polish Scientific Publishers and Springer-Verlag, Warszawa 1990. xiv+746 pp.

[7] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR 1757192

[8] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[9] A. Weil, L'arithm´etique sur les courbes alg´ebriques, *Acta Math.* **52** (1929), 281–315. Also OEuvres Scientifiques – Collected Papers. Vol. I, Corrected Second Printing, Springer-Verlag, New York–Heidelberg–Berlin 1980, 11–45.

[10] A. Weil, Sur un th´eor'eme de Mordell, *Bull. Sc. Math.* (2) **54** (1929), 182–191. Also OEuvres Scientifiques–Collected Papers. Vol. I, Corrected Second Printing, Springer-Verlag, New York– Heidelberg–Berlin 1980, 47–56.

[11] X. Wu, *Topics in Arithmetic Geometry: Arithmetic Heights and Mordell-Weil's Theorem* Part I

Email address: `xiaorunw@princeton.edu`