Height functions and the Mordell-Weil theorem

Padmavathi Srinivasan

Week 5

Starting from today's lecture, we will exclusively work with logarithmic heights.

Theorem 1 (Mordell-Weil)**.** *Let E/K be an elliptic curve defined over a number field K. Then $E(K)$ is a finitely generated abelian group. In other words, staring with a finite set of points in $E(K)$, and iterating the construction using secant and tangent lines, one can generate all points in $E(K)$.*

There are two key steps in the proof of the Mordell-Weil theorem. The first step, commonly referred to as the Weak Mordell-Weil theorem is to show $E(K)/2E(K)$ is finite. Note that this step alone is not enough since there are abelian groups A that are not finitely generated for which $A/2A$ is finite, for example $A = \mathbb{Q}$. The second step is deducing the Mordell-Weil theorem from its weak version and is commonly referred to as the "descent" step for reasons that will become apparent below. The descent step crucially uses the theory of heights of points on elliptic curves. Defining the canonical height function $\hat{h}_E \colon E(K) \to \mathbb{R}$ and understanding how it interacts with the group structure of $E(K)$ is the main goal of today's lecture.

Definition 2. The Weil height function of an elliptic curve E defined over a number field K is the function[1]

$$\begin{aligned} h_E \colon E(\overline{\mathbb{Q}}) &\to \mathbb{R} \\ P &\mapsto h(x(P)) \end{aligned}$$

Lemma 3. *Northcott property The number of points of $E(\overline{\mathbb{Q}})$ of bounded height and bounded degree is finite.*

Proof. This is an immediate consequence of the Northcott property of heights of algebraic numbers, since for each value of the x-coordinate on E, there are at most two values of y-coordinate, so once the possibilities for the x-coordinate are bounded, so are the possibilities for the y-coordinate. □

We would like to understand how the height function defined above interacts with the group law on the elliptic curve. We will first introduce the big-O notation for comparing real-valued functions on a set whose difference is bounded. This will be used throughout the rest of this lecture.

[1] One can replace the function x below by an arbitrary element of $K(x)$ and define an analogous height function. The new height function one obtains this way is closely related to the one corresponding to the one above, so we stick to the height function x for simplicity.

Heights on Abelian Varieties

The Quadratic Growth of the Height on Abelian Varieties

We illustrate with the elliptic curve and point

$$E : y^2 = x^3 + x + 1 \qquad \text{and} \qquad P = (0, 1).$$

Here is a table of $H(x(nP))$ for $n = 1, 2, \ldots, 25$.

1	1
2	2
3	13
4	36
5	685
6	7082
7	196249
8	9781441
9	645430801
10	54088691834
11	23545957758733
12	3348618159624516
13	3438505996705270765
14	2389279734043328028530
15	3568842156502352911081681
16	9147174028201584695660404993
17	40437302897155037003168469209281
18	144041052884595077187155035625188225
19	4077551427539061268365818617070082487981
20	29247742836717181569573123126609380958628633
21	1644662183623605030943992459758717959368038089933
22	76795559807444450146033952048248025474377706486132570
23	6037390795706541540397642739132383429233648456214266105001
24	816297679393916005694837838808362431503501229559444925278681793
25	242513738949178952234806483689465816559631390124939658301320990605073
26	47803232530993255659471421491008524334965293857886857075847338386784976289
27	67559659782039617237841184516992302782851604142385500859648938761010393239431661
28	32014345486637038681521545788678891610665676156825092102996356573331436095404542962201
29	75366079100860358183774143789438882594269554344230013075428451465317687946832468865183904333
30	235596097713466330738098972552422422374156906907547045290688341377958875910979032848694872594995042
31	949929776724866709094954536710367778326401614961417743163923974793524931042092311077415673676701373662241
32	6939337780803547166840419022721964472182663632045063388197164628060008767530358928827755424306465309623700644865
33	138560009627230805680861712729089150246171433367872626810509092219015283874452951868081163892328387927559567336088640513
34	1470496183658794212496122961743692131111461785062102204982019653166220314029845380022856443720777836633186409902489575338782721
35	107010592458999940561955702180302050658481740392774624430340775789803872514791716886258854994198364978765941985457904860326401460918221

Notice the parabolic shape, reflecting the quadratic growth in the number of digits.

An Introduction to Height Functions – 14–

Definition 4. Suppose S is a set and f, g are two functions $S \to \mathbb{R}$. We write $f = g + O(1)$ if there are constants C_1, C_2 such that for all $s \in S$, we have

$$C_1 \leq f(s) - g(s) \leq C_2.$$

The main theorem connecting the height function h_E and the group law on E is the following almost parallelogram law.

Theorem 5. [Sil09, Chapter 8, Theorem 6.2] *Let E be an elliptic curve over a number field K. Then for all $P, Q \in E(\overline{\mathbb{Q}})$, we have*

$$h_E(P + Q) + h_E(P - Q) = 2h_E(P) + 2h_E(Q) + O(1), \tag{1}$$

where the implied constants in $O(1)$ depend on E, but are independent of the pair of points P, Q. In particular, it follows that for any integer $m \in \mathbb{Z}$, we have

$$h_E(mP) = m^2 h_E(P) + O(1), \tag{2}$$

where the implied constants in the $O(1)$ notation depend only on E and m and not on the point P.

Suggested exercises 6. Deduce 1 from 2 and vice versa.

The exponent 2 in the expression $h_E(mP) = m^2 h_E(P) + O(1)$ is illustrated in the parabolic shape of the heights of x-coordinates above. (This graph is from [Sil06].) We temporarily postpone the proof of this theorem and will first show how one can carry out the descent step in the proof of the Mordell-Weil theorem from the theorem above. The descent step is even easier using the theory of canonical heights of elliptic curves, which obeys an exact parallelogram law instead of an almost parallelogram law.

Definition 7. (Tate) The canonical or Néron-Tate height on an elliptic curve E over a number field K is the function[2]

$$\begin{aligned}\hat{h}_E\colon E(\overline{\mathbb{Q}}) &\to \mathbb{R}\\ P &\mapsto \lim_{N\to\infty} \frac{h_E(2^N P)}{2\cdot 4^N}\end{aligned}$$

Proposition 8. [Sil09, Chapter 8, Proposition 9.1] *The canonical height function is well-defined, i.e., the limit in the definition of the canonical height function exists.*

Proof. We will show that the sequence $4^{-N}h_E(2^N P)$ is Cauchy. Theorem 5 with $m = 2$ tells us that there is a constant C such that for any Q in $E(\overline{\mathbb{Q}})$,

$$|h_E(2Q) - 4h_E(Q)| \leq C.$$

Let $N \geq M \geq 0$. We will repeatedly use the inequality above applied to the sequence of points $Q = 2^M P, 2^{M+1}P, \ldots, 2^{N-1}P$ below to show

$$|4^{-N}h_E(2^N P) - 4^{-M}h_E(2^M P)| \leq 4^{-M}C. \tag{3}$$

We have

$$\begin{aligned}|4^{-N}h_E(2^N P) - 4^{-M}h_E(2^M P)| &= \left|\sum_{n=M}^{N-1}(4^{-n-1}h_E(2^{n+1}P) - 4^{-n}h_E(2^n P))\right|\\ &\leq \sum_{n=M}^{N-1}(4^{-n-1}|h_E(2^{n+1}P) - 4h_E(2^n P))|\\ &\leq \sum_{n=M}^{N-1}4^{-n-1}C\\ &\leq 4^{-M}C.\end{aligned}$$

□

Theorem 9. *The canonical height function $\hat{h}_E\colon E(\overline{\mathbb{Q}}) \to \mathbb{R}$ satisfies the following properties:*

(a) *(Northcott) $|2\hat{h}_E - h_E|$ is a bounded function on $E(\overline{\mathbb{Q}})$. Hence, the set of points of $E(\overline{\mathbb{Q}})$ with bounded canonical height is finite.*

(b) *(Parallelogram law) Let $P, R \in E(\overline{\mathbb{Q}})$ be any two points of $E(\overline{\mathbb{Q}})$. Then, we have*

$$\hat{h}_E(P+R) + \hat{h}_E(P-R) = 2\hat{h}_E(P) + 2\hat{h}_E(R). \tag{4}$$

In particular, for any positive integer m, we have

$$\hat{h}_E(mP) = m^2\hat{h}_E(P) \quad \text{(canonicity)}, \tag{5}$$

and

$$\hat{h}_E(P+R) \leq 2\hat{h}_E(P) + 2\hat{h}_E(R). \tag{6}$$

[2]For the height h_f associated to an arbitrary even rational function $f \in K(x)$, the expression on the right hand side gets replaced by $\frac{h_E(2^N P)}{\deg(f)\cdot 4^N}$. The limiting value can be shown to be independent of choice of f.

(c) *(Uniqueness) Any function* $\hat{h}'\colon E(\overline{\mathbb{Q}}) \to \mathbb{R}$ *satisfying a and Equation 5 for any one integer* $m \geq 2$ *is equal to* $\hat{h}_E$.

Proof. Taking $M = 0$ and letting $N \to \infty$ in Equation 3 proves part a. Part b can be deduced from Theorem 5 and Definition 7 as follows. Replace P and Q in Theorem 5 by $2^N P$ and $2^N Q$, divide both sides by $2 \cdot 4^N$ and take the limit as $N \to \infty$ – this gets rid of the implied constants coming from the $O(1)$ term and converts the almost parallelogram law to an exact parallelogram law. The equality $\hat{h}_E(mP) = m^2 \hat{h}_E(P)$ can be proved by induction on m. Inequality 6 follows from the equality 4 since $\hat{h}_E(P - R) \geq 0$.

For part c, consider the function $g = \hat{h}' - \hat{h}_E$. We want to show that g is identically 0. On the one hand, since both $\hat{h}'$ and $\hat{h}_E$ satisfy a, it follows that their difference g is a bounded function on $E(\overline{\mathbb{Q}})$. On the other hand, if there is a point P such that $g(P) \neq 0$, then subtracting equation 5 for $\hat{h}'$ and $\hat{h}_E$ tells us that $g(mP) = m^2 g(P)$, and hence g is an unbounded function if $m \geq 2$, which is a contradiction. Hence g must be identically zero, or equivalently, that $\hat{h}' = \hat{h}_E$. □

Whenever we have a canonical height function on a group (i.e. a height function that plays well with the group law and obeys an equation like 5), we get a corresponding nice characterization of points of lowest height –

Corollary 10. *Let* $P \in E(\overline{\mathbb{Q}})$. *Then* $\hat{h}_E(P) \geq 0$. *Furthermore* $\hat{h}_E(P) = 0$ *if and only if* P *is a torsion point.*

Proof. $\hat{h}_E(P)$ is a limit of non-negative values and is therefore also non-negative. If P is a torsion point, then the set of values $h_E(2^N P)$ as N varies is bounded, and therefore $\hat{h}_E(P) = \lim_{N\to\infty} 2^{-1} 4^{-N} h_E(2^N P) = 0$. If $\hat{h}_E(P) = 0$ and P is defined over a finite extension L of K, then the set of points $\{P, 2P, 3P, \ldots\}$ is a set of points of bounded height (since $\hat{h}_E(mP) = m^2 \hat{h}_E(P) = 0$ for any integer m by canonicity) and bounded degree (all multiples of P are defined over the same number field L), and by the Northcott property is finite. This means there are $N > M \geq 0$ such that $NP = MP$, or in other words $(N - M)P = O$. □

Remark 11. Given Corollary 10, one may wonder if there is an analogous Lehmer type conjectural lower bound on the height of a non-torsion point on an elliptic curve E. See [Sil09, Chapter 8, Conjecture 9.9] for such a conjectural statement, where the shape of the lower bound of the height of a nontorsion point depends on some naturally associated invariants measuring the complexity of the elliptic curve E, such as the height of the j-invariant and the valuation of the minimal discriminant of E. (See Silverman's book for the definitions of these invariants.)

Theorem 12 (Descent)**.** *Assume that* $E(K)/2E(K)$ *is finite, and let* $P_1, P_2, \ldots, P_r$ *be a finite set of coset representatives for* $E(K)/2E(K)$. *Then Theorem 9 implies that the set*

$$S := \{R \in E(K) \ : \ \hat{h}_E(R) \leq \max_i \hat{h}_E(P_i)\},$$

is finite and that it generates $E(K)$.

Proof. The set S is finite by the Northcott property for $\hat{h}_E$ in Theorem 9. Now let G be the subgroup of $E(K)$ generated by the set S. We want to show that $G = E(K)$. Suppose this is not true. Let P in $E(K)$ be an element of smallest height that is outside G. We will use the properties of $\hat{h}_E$ from Theorem 9 to produce an element R in $E(K)$ outside G of even smaller height, which will be a contradiction. (This explains the name "descent" for this step.)

Since $P_1, P_2, \ldots, P_r$ is a complete set of coset representatives for $E(K)/2E(K)$, we may write $P = P_i + 2R$ for some i between 1 and r and for some R in $E(K)$. Using the parallelogram law for $\hat{h}_E$ in Theorem 9, we compute

$$\begin{aligned} 4\hat{h}_E(R) &= \hat{h}_E(2R) \\ &= \hat{h}_E(P - P_i) \\ &\leq 2\hat{h}_E(P) + 2\hat{h}_E(P_i) \\ &< 4\hat{h}_E(P) \qquad\qquad \text{since } P_i \in S \text{ and } P \notin S. \end{aligned}$$

□

We now return to the proof of the almost parallelogram law. The proof involves some explicit algebra using formulas for the group law of the elliptic curve. The third main feature of height functions that is crucial in this proof is the

"functoriality of heights under morphisms of projective spaces."

Proposition 13. [Sil09, Chapter 8, Theorem 5.6] *Suppose $F :: \mathbb{P}^N \to \mathbb{P}^M$ is a morphism of degree d over a number field K, i.e.*

$$F(P) = [f_0(P) \colon \ \ldots \colon f_M(P)],$$

where the f_i are homogeneous polynomials of degree d in $N+1$ variables with coefficients in the field K that have no common zeroes in $\overline{\mathbb{Q}}^{N+1} \setminus (0, 0, \ldots, 0)$. Then there are constants C_1, C_2 depending only on F and not on P such that

$$dh(P) + C_1 \leq h(F(P)) \leq dh(P) + C_2,$$

where the implied constants in the $O(1)$ depend only on F and not on P.

We will prove this proposition in the next lecture, but note that we already saw such an instance of this functoriality when we compared two different definitions of the height of a Pythagorean triple all the way back in Lecture 1! The relevant degree 2 morphism in question was the parametrization map we used to make a complete list of all Pythagorean triples –

$$\begin{aligned} &F \colon \mathbb{P}^1 \to \mathbb{P}^2 \\ &[p : q] \mapsto [q^2 - p^2 : 2pq : q^2 + p^2]. \end{aligned}$$

A dynamical analogue of an elliptic curve

Functoriality of heights under morphisms of projective spaces is also the key property that lets one define a canonical height function in the dynamical setting of a self-map $f : \mathbb{P}^n \to \mathbb{P}^n$. In the dynamical setting, iteratively doubling a starting point P on an elliptic curve is replaced by iteratively applying the morphism f to a point P in $\mathbb{P}^n$. A good reference for learning about the arithmetic of dynamical systems is [?SIlverman2]. For an integer $N \geq 1$, let $f^{\circ N} : \mathbb{P}^n \to \mathbb{P}^n$ be the morphism obtained by composing f with itself N times. If f has degree d, then $f^{\circ N}$ has degree d^N.

Definition 14. Suppose $f : \mathbb{P}^n \to \mathbb{P}^n$ is a morphism of degree $d \geq 2$ defined over a number field K as in Proposition 13. The canonical dynamical height associated to f is the function

$$\begin{aligned} \hat{h}_f \colon \mathbb{P}^n(\overline{\mathbb{Q}}) &\to \mathbb{R} \\ P &\mapsto \lim_{N\to\infty} \frac{h(f^{\circ N}(P))}{d^N}. \end{aligned}$$

Lemma 15. *The dynamical canonical height is well-defined, i.e., the limit above exists.*

Proof. The proof is identical to the proof of Proposition 8. Proposition 18 a implies there is a constant C such that

$$|h(f(P)) - h(P)| \leq C$$

for all P in $\mathbb{P}^n(\overline{\mathbb{Q}})$. The replacement for the inequality 3 in Proposition 8 is the following analogous inequality for $N > M \geq 0$ proved using a telescoping sum and geometric series argument:

$$\left| \frac{h(f^{\circ N}(P))}{d^N} - \frac{h(f^{\circ M}(P))}{d^M} \right| \leq \frac{C}{(d-1)d^M}. \tag{7}$$

□

Suggested exercises 16. Prove the inequality 7 and conclude that the sequence $\frac{h(f^{\circ N}(P))}{d^N}$ is Cauchy if $d \geq 2$ and hence converges.

The analogue of the torsion points on elliptic curves are the pre-periodic points for a rational map. These are the points whose orbit under f eventually enters a cycle.

Definition 17. Let $f \colon \mathbb{P}^n \to \mathbb{P}^n$ be a morphism defined over a number field K. A point P in $\mathbb{P}^n(\overline{\mathbb{Q}})$ is a is periodic point for f if there exists $N > 0$ such that $f^{\circ N}(P) = P$. A point P in $\mathbb{P}^n(\overline{\mathbb{Q}})$ is a pre-periodic point for f, if there exist integers $N > M \geq 0$ such that $f^{\circ N}(P) = f^{\circ M}(P)$.

Theorem 18. *Let $f : \mathbb{P}^n \to \mathbb{P}^n$ be a morphism of degree $d \geq 2$.*

(a) *$\hat{h}_f(P) = h(P) + O(1)$, where the implied constants in $O(1)$ are independent of the point P in $\mathbb{P}^n(\overline{\mathbb{Q}})$.*

(b) *(Canonicity) $\hat{h}_f(f(P)) = d\hat{h}_f(P)$.*

(c) *The function $\hat{h}_f$ is uniquely determined by properties a and b.*

(d) *$\hat{h}_f(P) \geq 0$ and $\hat{h}_f(P) = 0$ if an only if P is a pre-periodic point for f.*

Proof. Part 7 follows from the inequality 7 the same way that Theorem 9 a follows from the inequality 3. Part b is immediate from the limiting definition:

$$\hat{h}_f(f(P)) = \lim_{N\to\infty} \frac{h(f^{\circ N}(f(P)))}{d^N} = d \lim_{N\to\infty} \frac{h(f^{\circ N+1}(P))}{d^{N+1}} = d\hat{h}_f(P).$$

Part d applies the Northcott property and the canonicity analogous to the proof of Corollary 10. We instead consider the set of points $\{f(P), f^{\circ 2}(P), f^{\circ 3}(P), \ldots, \}$. Fill in the details! □

Suggested exercises 19. Fill in the details of the proof of Theorem 18.

Remark 20. In fact, the canonical height on an elliptic curve (up to a constant multiple) is equal to the canonical height of the x-coordinate for the corresponding Lattés map $\mathbb{P}^1 \to \mathbb{P}^1$ that expresses the x-coordinate of $2P$ as a degree 4 rational function evaluated at the x-coordinate at P.

Back to elliptic curves

For the almost parallelogram law, we will also need the following comparison, which is a generalization of the comparison inequality between two different height functions for an algebraic number that we proved in Lecture 2. Let $\alpha_1, \ldots, \alpha_n$ be any n algebraic numbers (not necessarily conjugate). Define

$$f(x) = a_0(x - \alpha_1)\ldots(x - \alpha_n) = a_0x^n + a_1x^{n-1} + \ldots + a_n.$$

Then

Proposition 21. [Sil09, Chapter 8, Theorem 5.9]

$$-n\log(2) + \sum_{i=1}^{n} h(\alpha_i) \le h([a_0 : \ \ldots : a_n]) \le (n-1)\log(2) + \sum_{i=1}^{n} h(\alpha_i)$$

Suggested exercises 22. Prove Proposition 21.

We will return to explicit algebra using formulas for the group law for the elliptic curve, together with Proposition 13 and Proposition 21 to prove the almost parallelogram law for h_E in the next lecture.

References

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑2, 3, 4, 5, 7

[Sil06] ———, *An Introduction to Height Functions* (2006). ↑2

[Sil07] ———, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. MR2316407 ↑