Height functions in Diophantine geometry

Padmavathi Srinivasan

Week 1

Diophantine geometry is the study of rational ($\mathbb{Q}$) or integral ($\mathbb{Z}$) solutions to a system of polynomial equations whose coefficients are in the integers. It is named after the Greek mathematician Diophantus who lived around 250 AD, but the subject as such is even older with some of the earliest records going as far back as 1800 BC. Historically famous examples include the study of the equation $x^2 + y^2 = z^2$ whose integer solutions are exactly the Pythagorean triples $(x, y, z) = (3, 4, 5), (5, 12, 13)$ etc. (integer side lengths of right triangles), the equation $x^n + y^n = z^n$ with $n \geq 3$ (the "Fermat curves" of Fermat's last theorem fame) with solutions $(x, y, z) = (1, 0, 1), (0, 3, 3)$ etc. A more recent example from 2019 that made a major newsplash with headlines such as "The answer to life, the universe, and everything" is a solution to the equation $x^3 + y^3 + z^3 = 42$.[1]

Identifying which integers can be written as a sum of three other integer cubes is an old challenge posed by Mordell in 1954.[2] By listing all the congruence classes of cubes of integers modulo 9, one immediately sees that $0, \pm 1 \mod 9$ are the only congruence classes containing cubes of integers, and therefore integers that are congruent to $\pm 4 \mod 9$ can never be written as a sum of three cubes. For integers in the remaining congruence classes such as the number 42, one might imagine searching for solutions by carrying out out a grid search – i.e., by plugging in small integer values for x, y and z (both positive and negative) and seeing if their cubes sum to 42, and slowly increasing the sizes of these integers. Such a search immediately yields a reasonably small solution for the similar equation $x^3+y^3+z^3 = 43$ (for e.g. $3^3 + 2^3 + 2^3 = 43$) that one may quickly find by hand, but I strongly recommend not attempting to solve $x^3 + y^3 + z^3 = 42$ the same way! Although a solution exists, such a search would take too long to finish even with the help of a computer without any additional insight to narrow the search space – the smallest solution found by Booker and Sutherland found in 2019 using massive parallel computations has 17 digits for each of x, y and z!

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3. \qquad (1)$$

It is still not known whether there are even more integer solutions to this equation out there – even if there are any, they are certainly very sparsely distributed and outside the range of values computers can access today. For example, it may very well be that the next solution has twice the number of digits!

[1] See also these Quanta articles – 33 and 42.

[2] See this Numberphile youtube playlist for a historical overview of the sum of three cubes problem and known methods and challenges.

The main driving questions in this area are the following. Given a system of polynomial equations over $\mathbb{Q}$,

1. How many integral/rational solutions does it have?
2. Is there a systematic and practical way to generate all the solutions?

For example,

Equation	**Some integral solutions**	**Number of solutions**
$x^2+y^2+z^2=0$	$(x,y,z)=(0,0,0)$	One
$x^2+y^2=z^2$	$(x,y,z)=(0,0,0),(3,4,5),(5,12,13),\cdots$	Infinitely many
$x^n+y^n=z^n, n\geq 3$	$(x,y,z)=(0,0,0),(1,0,1),(0,3,3),\cdots$	Infinitely many, but, every solution has at least one entry that is 0
$x^3+y^3+z^3=42$	See 1	Unknown!

Of particular interest in this course, are the polynomial equations that define "elliptic curves".

Definition 1 ([Sil09][p.42,§ III.I)**.**] An elliptic curve E over $\mathbb{Q}$ is a curve defined by an equation of the form

$$y^2=x^3+Ax+B,$$

where A and B are in $\mathbb{Q}$, and such that the number $\Delta := -16(4A^3+27B^2)$ is nonzero.

The equation $y^2=x^3+Ax+B$ is called a Weierstrass equation for the elliptic curve E. The associated number $\Delta := -16(4A^3+27B^2)$ is called the discriminant of the Weierstrass equation. The discriminant is the analogue of the quantity b^2-4ac for the quadratic polynomial ax^2+bx+c – the quantity $-16(4A^3+27B^2)$ is zero precisely when the cubic x^3+Ax+B has repeated roots. There is a wonderful online database of these curves in the LMFDB (L-functions and modular forms database) that I strongly encourage you all to explore as you familiarize yourself with these objects! (The database has helpful clickable definitions of interesting invariants associated to these curves, so is particularly user-friendly for beginners!) Here are some examples of elliptic curves and some of their rational solutions from the LMFDB.

Clickable equation	**Some rational solutions**	**Number of solutions**
$y^2=x^3+4$	$(x,y)=(0,\pm 2)$	Two
$y^2=x^3-x^2+x$	$(x,y)=(0,0),(1,\pm 1)$	Three
$y^2=x^3-108$		None
$y^2=x^3-x+1$	$(x,y)=(0,\pm 1),(1,\pm 1),(-1,\pm 1),\ldots$	Infinitely many
$y^2=x^3+x+1$	$(x,y)=(0,\pm 1),(\frac{1}{4},\pm\frac{-9}{8}),(72,\pm 611)\ldots$	Infinitely many
$y^2=x^3-7x+10$	$(x,y)=(1,\pm 2),(3,\pm 4)\ldots$	Infinitely many

[3] As a warmup to showing how we may generate more rational solutions to an elliptic curve starting from a small number of solutions, we will first illustrate how we can systematically generate all Pythagorean triples starting from the single triple $(-1, 0, 1)$ using some geometry.

1 Generating Pythagorean triples – using geometry!

The only solution in $\mathbb{Z}^3$ to $x^2 + y^2 = z^2$ with $z = 0$ is $(x, y, z) = (0, 0, 0)$. From now on, we will focus on finding solutions where $z \neq 0$. Also note that if (x, y, z) is a solution to $x^2 + y^2 = z^2$, then so is (cx, cy, cz) for any integer c. So from now on we will further focus on finding solutions where the greatest common divisor of x, y and z is 1.

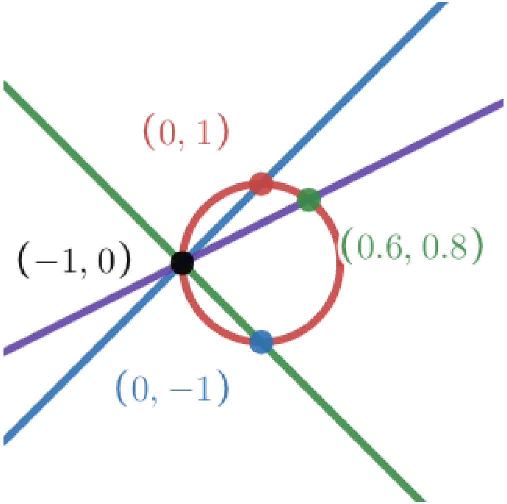
Observation 1: There is a bijection of sets:

$$\begin{aligned} \{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + y^2 = z^2,\ z \neq 0,\ \gcd(x, y, z) = 1\} &\longleftrightarrow \{(u, v) \in \mathbb{Q}^2 \mid u^2 + v^2 = 1\}. \\ (x, y, z) &\rightarrow (x/z, y/z) \\ (uz, yz, z) &\leftarrow (u, v), \end{aligned}$$

where z is the least common multiple of the denominators of u and v. So Pythagorean triples correspond to points on the unit circle where both coordinates are in $\mathbb{Q}$. For example, the triple $(x, y, z) = (3, 4, 5)$ corresponds to the point on the unit circle $(u, v) = (3/5, 4/5)$.

Observation 2: Let P_0 be the point corresponding to $(u, v) = (-1, 0)$. The line joining P_0 and any other point P on the unit circle with rational coordinates has rational slope.

Point P	**Slope of line joining** P_0 **and** P
$(1, 0)$	0
$(0, 1)$	1
$(0, -1)$	-1
$(3/5, 4/5)$	$1/2$



Observation 3: Conversely, we will show that any line through P_0 with rational slope t intersects the unit circle at one other point P, which also has rational coordinates. We will

[3] Note that all elliptic curves possess the symmetry $(x, y) \mapsto (x, -y)$, i.e. if (x, y) is a solution to $y^2 = x^3 + Ax + B$, so is $(x, -y)$. So the rational solutions with $y \neq 0$ come in pairs. The curves $y^2 = x^3 + 4$ and $y^2 = x^3 - 108$ are special since they possess additional symmetries, given by $(x, y) \mapsto (\omega x, y)$ where ω is a cube root of unity in $\mathbb{C}$. Elliptic curves possessing such additional symmetries are called CM elliptic curves (CM = Complex Multiplication). These are the "special points" described in some of the AWS course outlines!

show using a direct computation that

$$P = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right),$$

and hence also has rational coordinates when t is rational. The line through P_0 with slope t in the (u,v)-plane is given by $v = t(u+1)$. The two points of intersection of this line with the unit circle can be obtained by substituting $v = t(u+1)$ back into the equation $u^2 + v^2 = 1$ and solving for u. Carrying this out, we get the quadratic equation

$$u^2 + t^2(u+1)^2 = 1,$$

which on rearranging becomes the following quadratic equation in the variable u:

$$(t^2+1)u^2 + 2t^2u + t^2 - 1.$$

Note that $u = -1$ is a root of this quadratic equation (since the point $P_0 = (-1,0)$ is in the intersection of the line and the unit circle!), and the sum of the two roots is $-2t^2/(t^2+1)$, and hence the other root is

$$u = \frac{-2t^2}{t^2+1} - 1 = \frac{1-t^2}{1+t^2}.$$

The corresponding v-coordinate is obtained by plugging this value of u back into $v = t(u+1)$ and this gives $v = \frac{2t}{1+t^2}$ and the formula above for P.

We can now generate more rational points on the unit circle by plugging in our favourite rational value of t into this formula for P. For example, plugging in $t = -1/2$ gives us the point $(3/5, -4/5)$. Going back to the original problem of generating Pythagorean triples, writing $t = a/b$ for integers a and b, we see this value of t corresponds to the infinite set of Pythagorean triples that can be obtained from the triple $(b^2 - a^2, 2ab, b^2 + a^2)$ by scaling all three coordinates by the same integer.

Take away: We can generate all points on the unit circle with rational coordinates (and hence all Pythagorean triples) starting from the *single rational point* $P_0 = (-1,0)$ and computing the intersection of a line through P_0 with *rational slope* with the unit circle.

2 Measuring complexity of solutions: height functions

Now that we know how to systematically generate all points on the unit circle with rational coordinates, we can ask more refined questions such as how many solutions there are of a given "size/complexity", and how points of a given "size" distribute on the unit circle. As we saw in the example $x^3 + y^3 + z^3 = 42$ earlier, even the smallest solution that is accessible by a computer search to some equations can be quite complex i.e. have a large number of digits, and even if this equation has more solutions, they might be sparse and spread apart. Any natural notion of size should have the property that there are only finitely many points of any given size – this is precisely what height functions are designed for. There is more than one natural definition of a height function in the context of solutions to $x^2 + y^2 = z^2$, and we describe two such definitions below.

2.1 Height of a rational number

Definition 2. The height $H(a/b)$ of a rational number a/b written in lowest form is

$$H(a/b) := \max(|a|, |b|).$$

The logarithmic height $h(a/b)$ of a/b is $h(a/b) := \log H(a/b) = \log \max(|a|, |b|)$.

The logarithmic height is roughly a measure of the number of digits to write down the number a/b. We record the following easy, but extremely important feature of this definition.

Lemma 3. *(Northcott property) There are only finitely many rational numbers of bounded height.*

Proof. More precisely, if $H(a/b) \leq N$ for some integer N, then $-N \leq a \leq N$ and $-N \leq b \leq N$, so there are at most $(2N+1)^2$ possibilities of a/b. □

In fact, there can be fewer than $(2N+1)^2$ rational numbers of height $\leq N$ due to cancellations between the numerator and denominator. By estimating the probability that two randomly chosen integers are coprime, one can show

$$\#\{a/b \in \mathbb{Q} : \; h(a/b) \leq N\} \sim \frac{12}{\pi^2} N^2 + O(N \log N) \text{ as } N \to \infty.$$

Extending this definition of height for rational numbers to more general "algebraic numbers" such as roots of unity, $\sqrt[3]{2}, \sqrt{5}$ etc. will be the focus of the next couple of lectures.

One way to measure the size of the Pythagorean triple given by $(b^2 - a^2, 2ab, a^2 + b^2)$ for some integers a and b is to simply take the height of the rational number a/b.

2.2 Height function on projective spaces

There is an alternate way to directly measure the size of a Pythagorean triple (x, y, z) without first parameterizing, i.e. rewriting it in the form $(b^2 - a^2, 2ab, a^2 + b^2)$. The definition we give below naturally extends to arbitrary tuples of coprime integers.

Definition 4. (Projective spaces) Fix $n \geq 1$. Define

$$\mathbb{P}^n(\mathbb{Q}) := \{(x_0, x_1, \ldots, x_n) \in \mathbb{Q}^{n+1} \setminus (0, 0, \ldots, 0)\}/\sim,$$

where $\sim$ is the equivalence relation that identifies $(x_0, x_1, \ldots, x_n)$ with $(y_0, y_1, \ldots, y_n)$ if

$$(y_0, y_1, \ldots, y_n) = (ax_0, ax_1, \ldots, ax_n)$$

for some nonzero element a in $\mathbb{Q}$. We will denote the equivalence class of $(x_0, x_1, \ldots, x_n)$ by $[x_0 : x_1 : \ldots : x_n]$.

One can analogously define the set $\mathbb{P}^n(K)$ for any field K, by replacing the field $\mathbb{Q}$ in the definition above with the field K throughout.

Suggested exercises 5. Using the unique factorization property of the integers, show that every point P of $\mathbb{P}^n(\mathbb{Q})$ has a representative $(x_0, x_1, \ldots, x_n)$ where $x_i \in \mathbb{Z}$ for every i and $\gcd(x_0, x_1, \ldots, x_n) = 1$, and this representative is unique up to scaling by ± 1.

Definition 6. Fix an integer $n \geq 1$, and let $(x_0, x_1, ..., x_n)$ be a representative of a point P of $\mathbb{P}^n(\mathbb{Q})$ such that $x_i \in \mathbb{Z}$ for every i and $\gcd(x_0, x_1, \ldots, x_n) = 1$. Define the height function $H \colon \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}$ and the logarithmic height $h \colon \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}$ as follows.

$$H(x_0 : x_1 : \ldots : x_n) := \max(|x_0|, |x_1|, \ldots, |x_n|).$$
$$h(x_0 : x_1 : \ldots : x_n) := \log \max(|x_0|, |x_1|, \ldots, |x_n|).$$

Lemma 7. *(Northcott property) Fix an integer $n \geq 1$. There are only finitely many points of $\mathbb{P}^n(\mathbb{Q})$ of bounded height.*

Proof. More precisely, there are at most $(2N+1)^{n+1}$ points of $\mathbb{P}^n(\mathbb{Q})$ of height $\leq N$. □

The new height of a Pythagorean triple (x, y, z) is simply $H([x : y : z])$. This new height function is an equally good way for measuring the complexity/size. [4] Systematically packaging various different definitions of height functions for the same underlying set of solutions, and understanding their relationship is achieved by the Weil height machine – this is a topic that we will return to at the very end of this lecture series if we have time. Estimating the number of rational solutions of bounded height for more general systems of equations, and understanding how these estimates are related to the underlying geometry of the solution sets is an active area of research today!

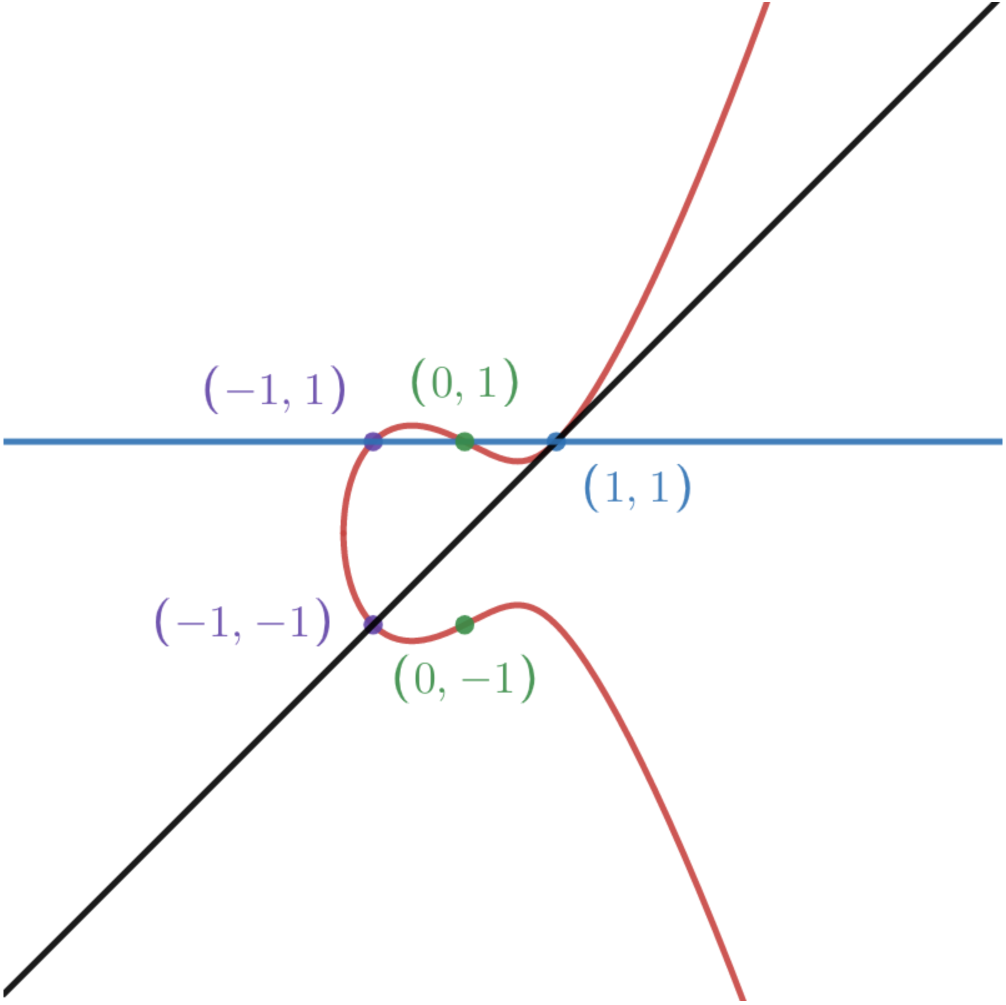
3 Generating rational points on elliptic curves

We are now interested in seeing if a similar geometric construction would help us systematically generate all rational solutions to an elliptic curve starting from a small number of known solutions. For example, if we take the elliptic curve E from the earlier table with defining equation $y^2 = x^3 - x + 1$, if we now draw a line between two of the known rational points $P_0 = (1, 1)$ and $P_1 = (0, -1)$ on E, i.e. the line with equation $y = 2x - 1$, and compute where it intersects the curve $y^2 = x^3 - x + 1$ by substituting for y in terms of x as before, we get the equation $(2x - 1)^2 = x^3 - x + 1$ and we see that this line intersects the curve at three distinct points. This time we end up having to solve the cubic equation $x^3 - 4x^2 + 3x = 0$, with two known solutions 0 and 1 (corresponding to the x-coordinates of P_1 and P_0). Since the sum of the three roots of the cubic is 4 (minus the coefficient of x^2), the third root is $x = 4 - (0 + 1) = 3$, and the corresponding y-coordinate is $y = 2 \cdot 3 - 1 = 5$, giving us the new solution $P_3 = (3, 5)$. Using the symmetry of the defining equation, under $(x, y) \mapsto (x, -y)$ we see that $P_4 = (3, -5)$ is also a solution.

In fact, we can even obtain the point P_1 from P_0 by iterating a similar construction starting with the single point P_0! (See figure 3.) We begin by computing the tangent line to the elliptic curve at P_0. This line has slope 1 (which we can compute by implicit differentiation), and so has equation $y = x$. It intersects the elliptic curve E at one more

[4] It is possible to estimate the number of rational solutions of bounded height using this new definition of a height function. The new estimate for points of height at most N turns out to be of the order of a constant times N up to a lower order error term. Although this estimate differs from the earlier estimate of $\frac{12}{\pi^2}N^2$, it is not altogether surprising – one can explain the difference from the "squares" in the parameterization $(q^2 - p^2, 2pq, p^2 + q^2)$ – your homework will help you prove these!

Figure 1: Some rational points on the elliptic curve $y^2 = x^3 - x + 1$



point P_5. To find P_5, this time we will have to solve the cubic polynomial $x^2 = x^3 - x + 1$, with 1 as a repeated root with multiplicity 2 and sum of three roots equal to 1 – this gives the point $P_5 = (-1, -1)$. Using the symmetry again gives us the point $P_6 = (-1, 1)$ on E. The horizontal line joining $(-1, 1)$ and the original point P_0 meets E also at $P_7 = (0, 1)$. Using the symmetry once again gives the point $P_1 = (0, -1)$.

More generally, one can show that this geometric construction gives the set of rational points on any elliptic curve the structure of an abelian group, where

$$P_1 + P_2 + P_3 \text{ is the identity} \Leftrightarrow P_1, P_2, P_3 \text{ lie on a line,}$$

for any three rational points P_1, P_2, P_3 on E, not necessarily distinct. For instance, associativity of the group law does not follow immediately from the description above and takes some work. For a proof, see [Sil09][Chapter 3, Proposition 2.2]. To see what the identity element is for this group, we need to "re-homogenize" the equation $y^2 = x^3 + Ax + B$ to a cubic equation in the three variables X, Y, Z where each monomial has degree 3. Formally, we substitute $x = X/Z, y = Y/Z$ analogously to the change of variables we made to pass from Pythagorean triples to points on the unit circle. Clearing denominators to get

$Y^2Z = X^3 + AX^2Z + BZ^3$. This time we see there are many solutions to this "rehomogenized" equation with $Z = 0$: they can all be obtained from the solution $(X, Y, Z) = (0, 1, 0)$ by scaling by an integer. We formally view this additional solution (unique up to scaling) as giving us a point O "at infinity" on this elliptic curve, and understand that this point lies on every vertical line in the (x, y) plane. So a line joining an arbitrary point P with O is a vertical line through P. At this point, it might be instructive to verify that O satisfies the axioms to qualify as the identity element, and that the inverse of a point $P = (x, y)$ is the symmetric point $(x, -y)$!

We can reinterpret the calculations above with the example $y^2 = x^3 - x + 1$ discussed above as saying:

$$\begin{aligned} P_1 + P_2 + P_3 &= O \\ P_3 + P_4 &= 0 \\ 2P_0 + P_5 &= O \\ P_5 + P_6 &= O \\ P_6 + P_7 + P_0 &= O \\ P_7 + P_1 &= O. \end{aligned}$$

On simplifying this sequence of equalities, we see that this $P_1 = 3P_0$.

Given an elliptic curve E with defining equation $y^2 = x^3 + Ax + B$, define the group $E(\mathbb{Q})$ of rational points by

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \ : y^2 = x^3 + Ax + B\} \cup \{O\}.$$

Suggested exercises 8. Verify that $(1, 1)$ is a point of order 4 on the elliptic curve $E_1\colon y^2 = x^3 - x^2 + x$, and that $(0, 2)$ is a point of order 3 on the elliptic curve $E_2\colon\ y^2 = x^3 + 4$.

At this point, it is natural to wonder if we can generate *all* rational points on the elliptic curve $E\colon y^2 = x^3 - x + 1$ starting from the single rational point $(1, 1)$ and iterating this construction of drawing tangent and secant lines and computing points of intersection with E. Or in other words, is $E(\mathbb{Q}) \cong \mathbb{Z}$ with generator $(1, 1)$? Miraculously, it turns out the answer is yes! The analogous finite generation statement for arbitrary elliptic curves over $\mathbb{Q}$ is one of the foundational theorems of the subject:

Theorem 9 (Mordell-Weil)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group for any elliptic curve E defined over $\mathbb{Q}$. In other words, staring with a finite set of rational points, and iterating the construction using secant and tangent lines, one can generate all points in $E(\mathbb{Q})$.*

The year 2022 marks the 100 year anniversary of this historic theorem. The theorem as stated above should rightly be attributed to Mordell. In this thesis in 1928, Weil greatly generalized Mordell's theorem to points on elliptic curves defined over more general number systems, and also to certain higher dimensional analogues of elliptic curves called "abelian varieties". [5] Although Mordell's theorem shows that the set of rational points is finitely generated, it does not give an algorithm for finding an explicit set of generators – this remains an important challenge in computational number theory today!

Here's a table of some elliptic curves and their corresponding Mordell-Weil groups $E(\mathbb{Q})$.

[5] See the article "Mordell's finite basis theorem revisited" by Cassels for a nice historical overview.

Clickable equation	$E(\mathbb{Q})$	**Generators for** $E(\mathbb{Q})$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 - x^2 + x$	$\mathbb{Z}/4\mathbb{Z}$	$(1, 1)$
$y^2 = x^3 - 108$	trivial	O
$y^2 = x^3 - x + 1$	$\mathbb{Z}$	$(1, 1)$
$y^2 = x^3 + x + 1$	$\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + x^2 + 4$	$\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(0, 2), (-2, 0)$
$y^2 = x^3 - 7x + 10$	$\mathbb{Z} \oplus \mathbb{Z}$	$(1, 2), (3, 4)$

There are algorithms to compute the torsion subgroup of $E(\mathbb{Q})$. The behaviour of the rank of the Mordell-Weil group as you vary over elliptic curves over $\mathbb{Q}$ remains relatively mysterious – whether there is a "largest possible rank" for an elliptic curve defined over $\mathbb{Q}$ is a topic of heated debate! The current record for largest rank is held by Noam Elkies who found 28 independent points on the following elliptic curve

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x$$
$$+34481611795030556467032985690390720374855944359319180361266008296291939448732243429.$$

Proving that the average rank is bounded as you vary over all elliptic curves over $\mathbb{Q}$ is one of the modern breakthroughs in the subject.

One of the key tools used in the proof of the Mordell-Weil theorem is the canonical height function $\hat{h}_E \colon E(\mathbb{Q}) \to \mathbb{R}$. (At this point, you can try and come up with a reasonable definition for a height function on $E(\mathbb{Q})$! Remember, any good definition must satisfy the Northcott property.) Defining the canonical height function and understanding how it interacts with the group structure of $E(\mathbb{Q})$ is one of the main goals for this course.

Suggested exercises 10. Verify that the doubling map for the elliptic curve $y^2 = x^3 + 1$ is given by

$$P = (x, y) \mapsto 2P = \left(\frac{x^4 - 8x}{4x^3 + 4}, \frac{2x^6 + 40x^3}{8y^3} \right).$$

Note that we cannot plug in the point $(-1, 0)$ on the curve into the formula above – can you explain why?

The map $f(x) = \frac{x^4-8x}{4x^3+4}$ is an example of a Lattès map. A Lattès map is a rational function (i.e. a ratio of two polynomials) that describes the x-coordinate of the point $2P$ in terms of the x-coordinate of P for some elliptic curve.

Suggested exercises 11. Compute the Lattès map corresponding to the elliptic curve $y^2 = x^3 + 2$. Let P be the point $(-1, 1)$ on this curve. Compute the formula for the x-coordinates of the points $2P, 4P, 8P, 16P$ by iteratively plugging them into the Lattes map for this curve – what do you observe about the growth of the number of digits in this sequence?

Suggested exercises 12. Try this exercise if you have access to one of the computing softwares Magma/Pari GP/SAGE. (Your wonderful TAs can help you run these experiments at office hours!) Open up the webpage of your favourite elliptic curve from this list of curves from the LMFDB of elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}$. Using the "Show command" option on the top right of the webpage you opened up, learn how to enter the elliptic curve and a generator P for the Mordell-Weil group into your chosen platform. Also compute the points $2P, 4P, 8P, 16P$ etc. using your chosen platform – what do you observe about the heights of the x-coordinates of these points? Repeat this experiment with a different elliptic curve from the list.

References

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

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