Height functions in Diophantine geometry

Polynomial equations	Integral ($\mathbb{Z}$)/ Rational ($\mathbb{Q}$) Solutions
$x^2 + y^2 = z^2$	= "Pythagorean triplets" (3, 4, 5). (5, 12, 13).
$x^n + y^n = z^n$, $n \geq 3$	(3, 0, 3), (0,1,1). → Only solutions

$$x^3 + y^3 + z^3 = 3$$

(x, y, z)

$= (1, 1, 1),$

$(4, -5, 4),$

$(4, 4, -5),$

$(-5, 4, 4),$

$?$

Any more???

In 1953, Mordell said *"I do not know anything about the integer solutions of* $x^3 + y^3 + z^3 = 3$ *beyond the existence of the four triples* $(1,1,1), (4,4,-5), (4,-5,4), (-5,4,4)$*; and it must be very difficult indeed to find out anything about any other solutions."*

Booker and Sutherland's 2019 computer search yielded one more – are there infinitely more solutions?

The answer to life, the universe, and everything

– available on Amazon!

$x^3+y^3+z^3=42$

The "smallest" solution to $x^3 + y^3 + z^3 = 42$ found by Booker-Sutherland (2019).
$(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42$.

DRIVING QUESTIONS IN DIO. GEO.

Given a system of poly. eqns./$\mathbb{Q}$,

1) How many integral / rational solutions does it have?

2) Is there a systematic way to generate all rat'l solns?

In this course, rational points on "elliptic curves"

<u>Defn</u>: An "elliptic curve" is a curve defined by an equation of the form

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}$$

$$\Delta = -16(4A^3 + 27B^2) \neq 0$$

Elliptic curves	Some ratl. solutions	# of solutions
$y^2 = x^3 + 4$	$(x,y) = (0, \pm 2)$ ←	These are all! Two
$y^2 = x^3 - 108$		None.
$y^2 = x^3 - x + 1$	$(x,y) = (0, \pm 1)$ $(1, \pm 1)$, $(-1, \pm 1)$, ...	Infinitely many solutions!

Question: Can we generate more soln to $y^2 = x^3 - x + 1$ from the known solutions?

§1 Warmup: Generating Pythagorean triples, using geometry.

GOAL: Solve $x^2+y^2=z^2$

with $(x,y,z) \in \mathbb{Z}^3$

Plug in $z=0 \Rightarrow x^2+y^2=0$

$\Rightarrow x=y=0$

From now on focus on solns with

$\boxed{z \neq 0}$.

(x, y, z) is a soln $\Rightarrow$ (cx, cy, cz) is also a soln for $c \in \mathbb{Z}$.

$(3, 4, 5) \xrightarrow{\times 2} (6, 8, 10)$

$ \xrightarrow{\times -1} (-3, -4, -5)$

Without loss of generality, look for solns with

$$\boxed{\gcd(x, y, z) = 1}$$

Observation 1 There is a bijection

$$\{(x,y,z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\} \mid \gcd(x,y,z)=1,\ x^2+y^2=z^2\}$$

(uz, vz, z) $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ (x,y,z)

$z = \mathrm{lcm}(\mathrm{denom}(u), \mathrm{dem}(v))$

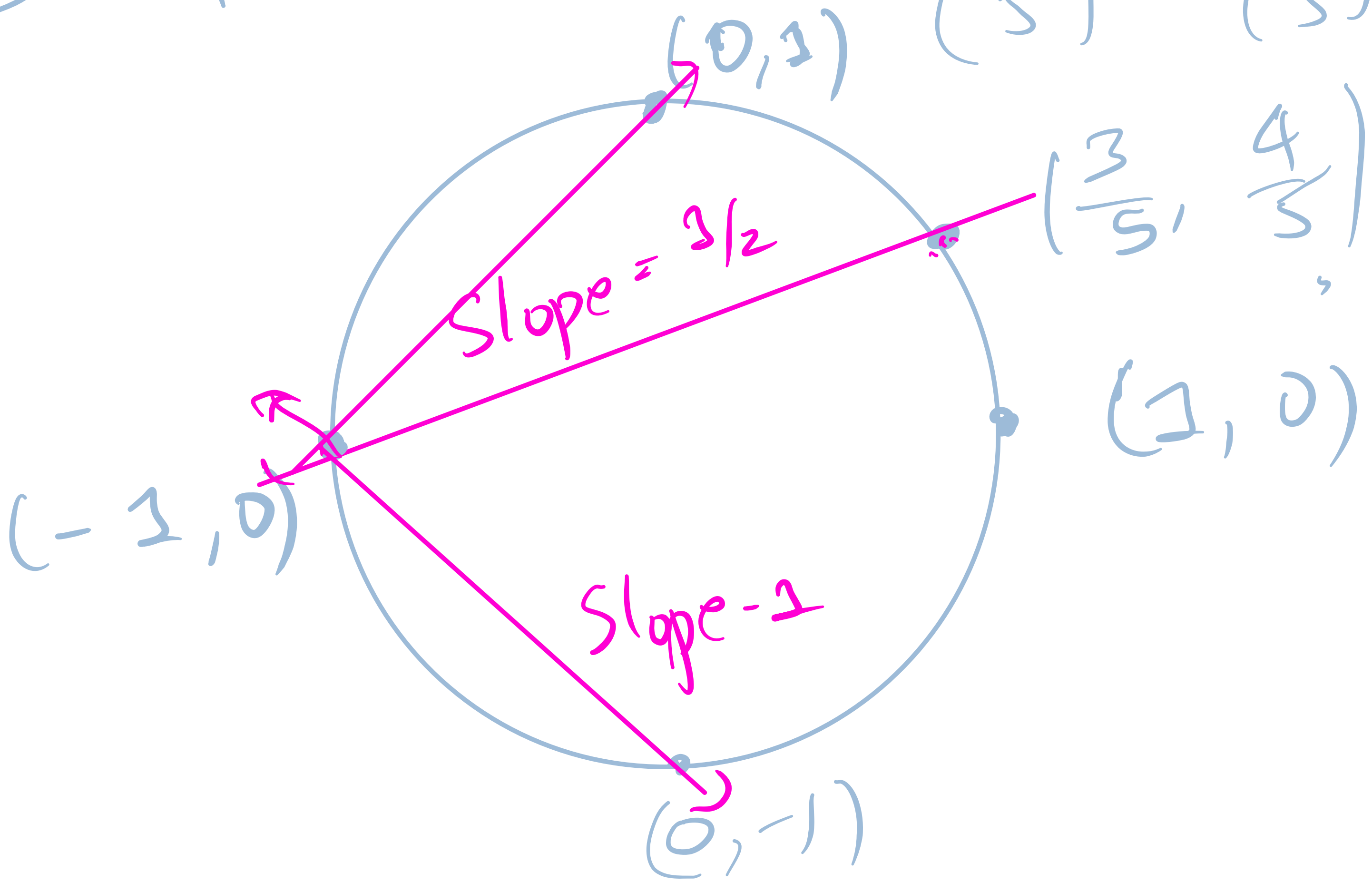
(u,v)

$$\{(u,v) \in \mathbb{Q}^2 \mid u^2+v^2=1\} \quad \left(\frac{x}{z}, \frac{y}{z}\right)$$

(x, y, z)

$$(3, 4, 5) \longrightarrow \left(\tfrac{3}{5}, \tfrac{4}{5}\right) = (u, v)$$

$$3^2 + 4^2 = 5^2 \rightsquigarrow \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$$



Observation 2: Line joining a rational pt. P with the fixed pt $P_0 = (-1,0)$ get a line with rational slope.

P	Slope of line joining P_0 & P
$(1,0)$	0
$(0,1)$	$\frac{1-0}{0-(-1)} = 1$

$(0, -1)$ $\quad = -1$

$\left(\frac{3}{5}, \frac{4}{5}\right)$ $\quad \dfrac{4/5 - 0}{3/5 - (-1)} = 1/2$

Observation 3: Conversely, every line with rational slope t through $P_0 = (-1, 0)$

intersects the unit circle

@ another rational pt.

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

$$P = \left(3/5, -4/5 \right)$$

t

$t = -1/2$

$-1/2$

Want: equation of line through $P_0 = (-1, 0)$ & slope t $\rightsquigarrow$ $\boxed{v = t(u+1)}$

Want: Point of intersection with $\boxed{u^2 + v^2 = 1}$

Substitute $v = t(u+1)$ into

$u^2 + v^2 = 1$

$$[t(u+1)]^2 + u^2 = 1$$

$$\Rightarrow t^2(u^2 + 2u + 1) + u^2 = 1$$

$$\Rightarrow \boxed{(t^2+1)u^2 + 2t^2 u + t^2 - 1 = 0}$$

Compare with $au^2 + bu + c = 0$

Sum of the two roots $= -\frac{b}{2a}$

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

Know $u=-1$ is a root!

($P_0=(-1,0)$ is on line & on circle)

$\therefore (t^2+1) - 2t^2 + (t^2-1) = 0$

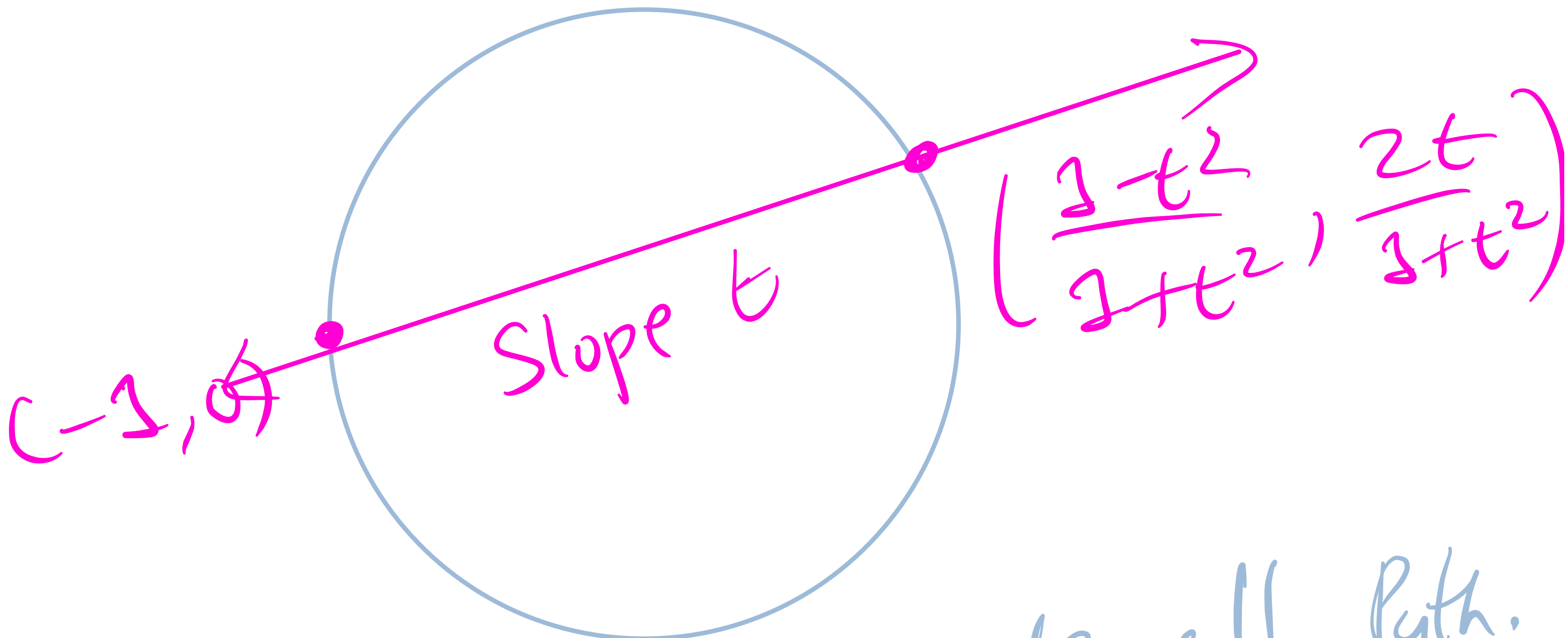
Solve for other root:

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

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

$$v = t(u+1) = t\left[\frac{1-t^2}{1+t^2}+1\right]$$

$$= \frac{2t}{1+t^2}$$



<u>TAKE AWAY</u>: Can generate <u>all</u> Pyth. triples / pts on unit circle by

taking a fixed point $P_0 = (-1, 0)$ & drawing a line of rational slope through P_0.

§2 Measuring complexity of solutions -- height functions

Want: # of solutions of bounded size/complexity to be finite.

Two natural notions of a height function for Pythagorean triples.

<u>Defn 1:</u> The <u>height</u> of a rat'l. # a/b, written in lowest form

$$H\left(a/b\right) = \max(|a|, |b|)$$

logarithmic height h:

$$h\left(a/b\right) = \log \max(|a|, |b|)$$

$h(a/b) \sim$ # of digits to write down a/b'

<u>Next lecture:</u> $h(\sqrt[3]{2}+1) = ??$

Height functions of "algebraic #s"

KEY PROPERTY (Northcott):

of rational #s of bounded height is finite.

Proof: If $H(a/b) \leq N$,

$-N \leq a \leq N \longrightarrow$ 2N+1 possible a-vals

$-N \leq b \leq N$

$$\#\{a/b : H(a/b) \le N\} \le (2N+1)^2$$

Height of Pythagorean triple

$$h(b^2-a^2, 2ab, b^2+a^2) = h(a/b)$$

$$t = a/b \rightsquigarrow \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \rightsquigarrow$$

$$[\underbrace{b^2-a^2}_{=x}, \underbrace{2ab}_{=y}, \underbrace{b^2+a^2}_{=z}]$$

$H(3,4,5) = H(1/2) =$

$\max(|1|, |2|) = 2$

There is a second definition of height (x,y,z) w/o first parametrizing Pythagorean triple $(b^2-a^2, 2ab, a^2+b^2)$.

Rmk:

Natural to study tuples of coprime integers

— — integers / $\sim$ scaling

$(3,4,5) \sim (6,8,10)$

Defn: Fix $n \geq 1$. Define projective n-space $\mathbb{P}^n$

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

$(x_0, x_1, \ldots, x_n) \sim (ax_0, ax_1, \ldots, ax_n)$

for any $a \neq 0$ $a \in \mathbb{Q}$

The equivalence class of $(x_0, x_1, \ldots x_n)$ will be denoted

$[x_0 : x_1 : \ldots : x_n]$.

Observe: every pt of $\mathbb{P}^n(\mathbb{Q})$ has a representative when $x_i \in \mathbb{Z}$

$$\gcd(x_0, x_1, \ldots, x_n) = 1$$

Ex: $n = 2$

$$[3, 4, 5] \sim [3/5, 4/5, 1] \sim [6, 8, 10]$$

$[3:4:5]$

<u>Defn:</u> The height function

$$H : \mathbb{P}^n(\mathbb{Q}) \longrightarrow \mathbb{R}$$

logarithmic height $\quad h : \mathbb{P}^n(\mathbb{Q}) \longrightarrow \mathbb{R}$

$$H([x_0 : x_1 : \dots : x_n]) = \max(|x_0|, |x_1|, \dots, |x_n|)$$

$\gcd(x_0, \dots x_n) = 1$

$x_i \in \mathbb{Z}$

Remk: $H(p/q) = H[p:q]$

$\mathbb{P}^1$

$h([x_0 : \dots : x_n]) = \log H([x_0 : \dots : x_n])$

Northcott property:

# of points of $\mathbb{P}^n(\mathbb{Q})$ of bounded ht is finite.

<u>Pf:</u> # of pts of $\mathbb{P}^n(\mathbb{Q})$ of

$\text{ht} \le N \quad \le \quad (2N+1)^{n+1}$

<u>Application.</u> The height of a Pythagorean triple is $H([x:y:z])$

$H([3:4:5]) = 5$

Remark: These two different ~~measures~~ definit'n of height functions are very closely related.

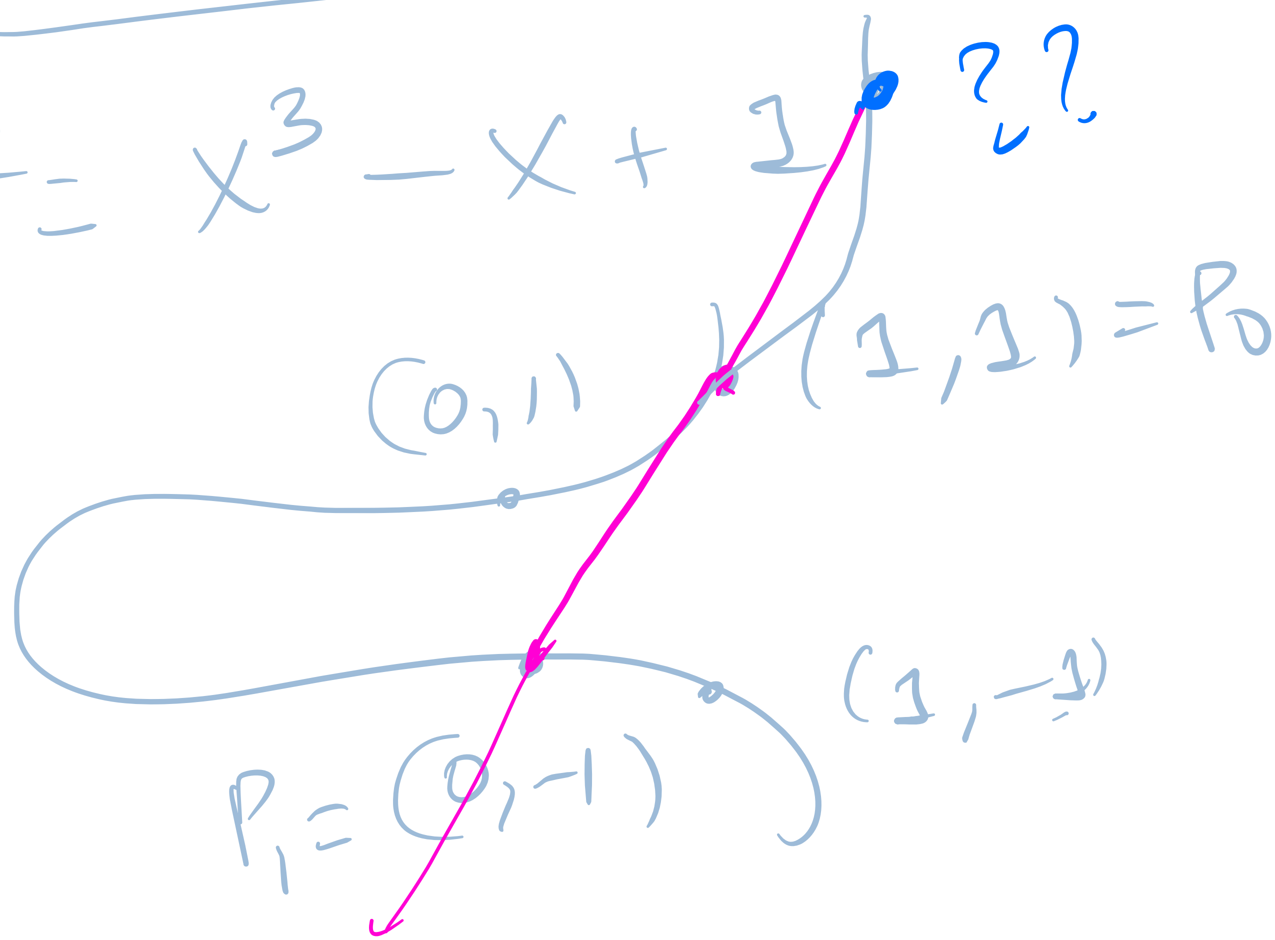
"Weil height machine"

$$\#\{a/b : H(a/b) \leq N\} \sim \frac{12}{\pi^2} N^2 \text{ as } N \to \infty$$

(Related to probability that 2 randomly chosen integers are coprime).

§3: Generating ratl. points on elliptic curves

$E: \; y^2 = x^3 - x + 1$



Draw line L joining

$P_0 : (1, 1)$ $\quad$ $P_1 : (0, -1)$

intersect the elliptic curve E

at one more point.

$$L: \ y = 2x - 1$$

$$E: \ y^2 = x^3 - x + 1$$

Substitute $y = 2x - 1$ into

$y^2 = x^3 - x + 1$

$(2x-1)^2 = x^3 - x + 1$

$\rightsquigarrow \quad x^3 - 4x^2 + 3x = 0$

Expand
rearrange

Know: $x = 0$, $x = 1$

are both solutions

Sum of 3 roots $= -(-4)$

$= 4$

$\Rightarrow$ Third root $= 4 - (0+1)$

$= 3 = x$

$y = 2x - 1 = 2 \cdot 3 - 1 = 5$

$(3, 5)$ is also a ratl-pt

on $y^2 = x^2 - x + 1$.

$(3, -5)$ is also a ratl pt.

Can set $P_1 = (0,-1)$

from just $P_0 = (1,1)$.

Fact: The set of rational soln. have a group structure

P_1, P_2, P_3 rat'l. points on $E(\mathbb{Q})$

(not necessarily distinct)

$P_1 + P_2 + P_3 = O \iff P_1, P_2, P_3$ lie on a line.

Identity?

$$y^2 = x^3 + Ax + B \xrightarrow{\text{Rehomogenize}} \left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 + \cdots$$

$$y = \frac{Y}{Z}, \quad x = \frac{X}{Z}$$

Clear denominator

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

$Z = 0 \rightsquigarrow X = 0$

$Y = $ any #

Identity element: $[0:1:0] \in \mathbb{P}^2(\mathbb{Q})$

Lies on every vertical line.

Inverse $P = (x, y)$

$$\downarrow$$

$$-P = (x, -y)$$

Proof of associativity $\rightsquigarrow$ See Silverman's books

$E: y^2 = x^3 - x + 1$, we could generate all points we know starting from just $P = (1,1)$

Mordell-Weil Theorem:

For any elliptic curve $E/\mathbb{Q}$, the group of rat'l. pts

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

$[0:1:0]$

is a finitely generated abelian group. This means, there is a way to generate all rat'l pts starting from a finite set of rat'l pts & iterating secant/tangent line construction.

Example:

$E_1: \ y^2 = x^3 - x + 1$

$E(\mathbb{Q}) \simeq \mathbb{Z}$

$(1, 1) \leftarrow 1$

$E_2: \ y^2 = x^3 + 4$

$E_2(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$

$(0, 2) \leftarrow 1$

$E_3: \; y^2 = x^3 - 7x + 10$

$$E_3(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z}$$

$(1,2) \leftarrow\!\shortmid (1,0)$

$(3,4) \leftarrow\!\shortmid (0,1)$

KEY TOOLS: for proving Mordell-Weil Theorem is the canonical ht fn.

$$\hat{h}_E : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$