Binary Quadratic Forms

↓

Two variables

Degree 2

Homogeneous

Example: $7x^2 + 5y^2$

Motivating question: Solutions of $F(x,y) = c$ in integers

Example: $31x^2 + 1 = y^2$

Euler's solution $x > 0$ $x = 273$

x as small as possible $y = 1520$

1990's, John Conway (1937 - 2020) NJ Visual approach to solving these equations

2-D Hops and Skips

Using vectors $(23,5)$ and $(14,3)$, which other vectors (a,b) can be written as their linear combination?

$$(23,5) = (14,3) + (9,2)$$

$$(14,3) = (9,2) + (5,1)$$

$$(9,2) = (5,1) + (4,1)$$

$$(5,1) = (4,1) + (1,0)$$

$$(4,1) = 4(1,0) + (0,1)$$

Another example: $(97,14)$ $(28,37)$

$$(97,14) = 3(28,37) + (13,-97)$$

$$(28,37) = 2(13,-97) + (2,231)$$

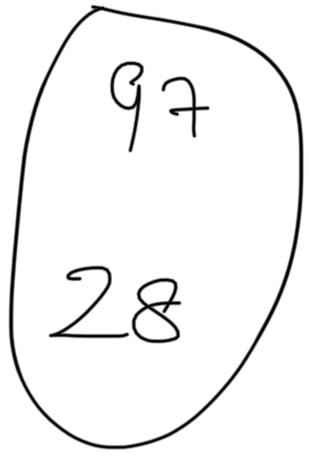
$$(13,-97) = 6(2,231) + (1,-1483)$$

$$(2,231) = 2(1,-1483) + (0,3197)$$

Can't get $(0,1)$ using these two vectors!

Coprime

Coprime



Coprime

Coprime

Where's the difference?

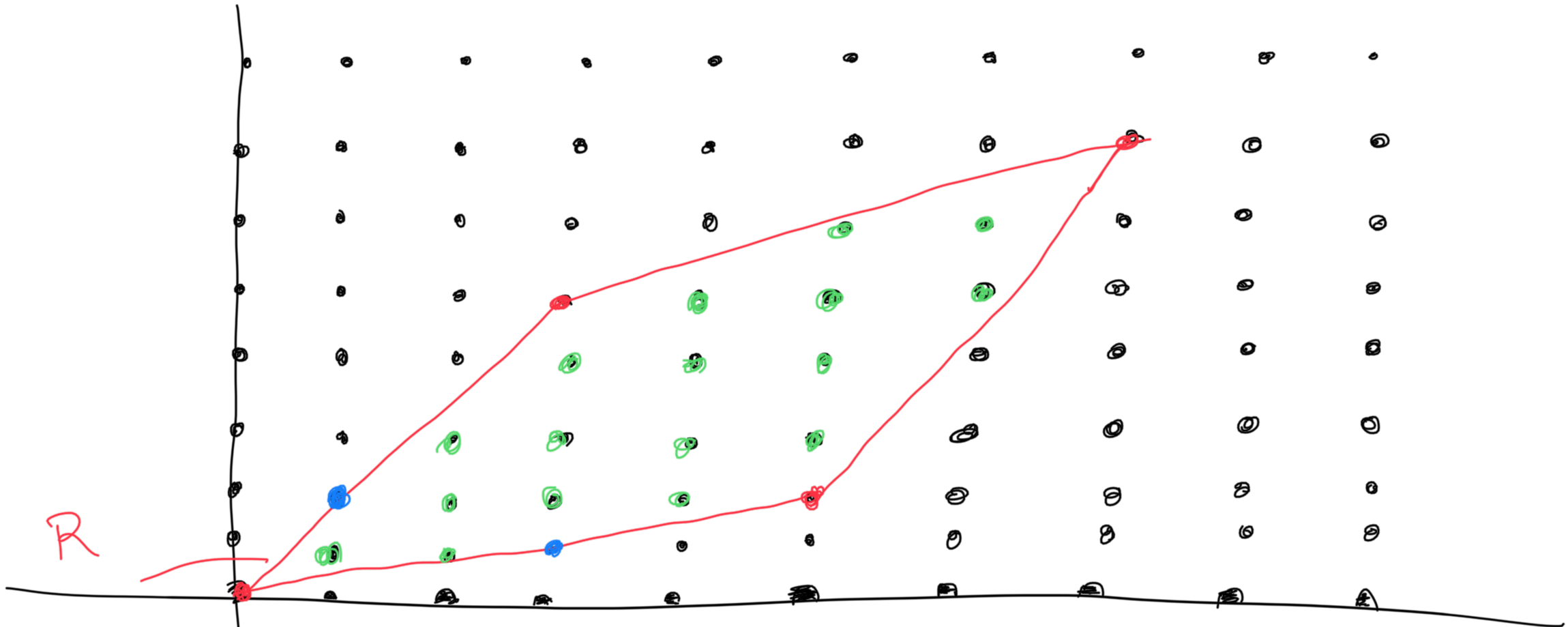
$$\begin{vmatrix} 23 & 5 \\ 14 & 3 \end{vmatrix} = -1$$

$$\begin{vmatrix} 97 & 14 \\ 28 & 37 \end{vmatrix} = 2553$$

Thm: The vectors (a,b) & (c,d) form a basis $\iff$ $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1$.

Pf: Step 1: (Pick's theorem)

Proof is (Reading Exercise !)



Area of R = 1 + No. of interior grid points + $\frac{1}{2}$ (No. of grid points crossed by edges)

(a,b) & (c,d) form a basis

$\iff$ there are no interior points

& points on edges

$\iff$ Area $= 1$

$\iff$ $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$ or $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = -1$

Some Observations

→ If (a, b) is one of basis vectors

then $GCD(a, b) = 1$

b/c there is some (c, d) such that

$$ad - bc = 1$$

or $ad - bc = -1 \Rightarrow a(-d) + bc = 1$

→ Given a vector (a,b) such that GCD $(a,b)=1$ you can always find another vector (c,d) such that $\{(a,b),(c,d)\}$ forms a basis.

By Euclidean algorithm!

$$3(1)-2(1)=1$$

$\{(3,2),(1,1)\}$ is a basis.

Some Terminology

→ (a,b) is called primitive

⟺ $\gcd(a,b) = 1$.

→ A pair $\pm(a,b)$ is called a lax vector.

→ A lax basis is an unordered pair $\{\pm v, \pm w\}$ of lax vectors.

Domain Topograph

Visualizing all primitive lax vectors, lax bases & their connections.

→ If $\{v, w\}$ is a basis, then

$\{v, v \pm w\}$ is a basis

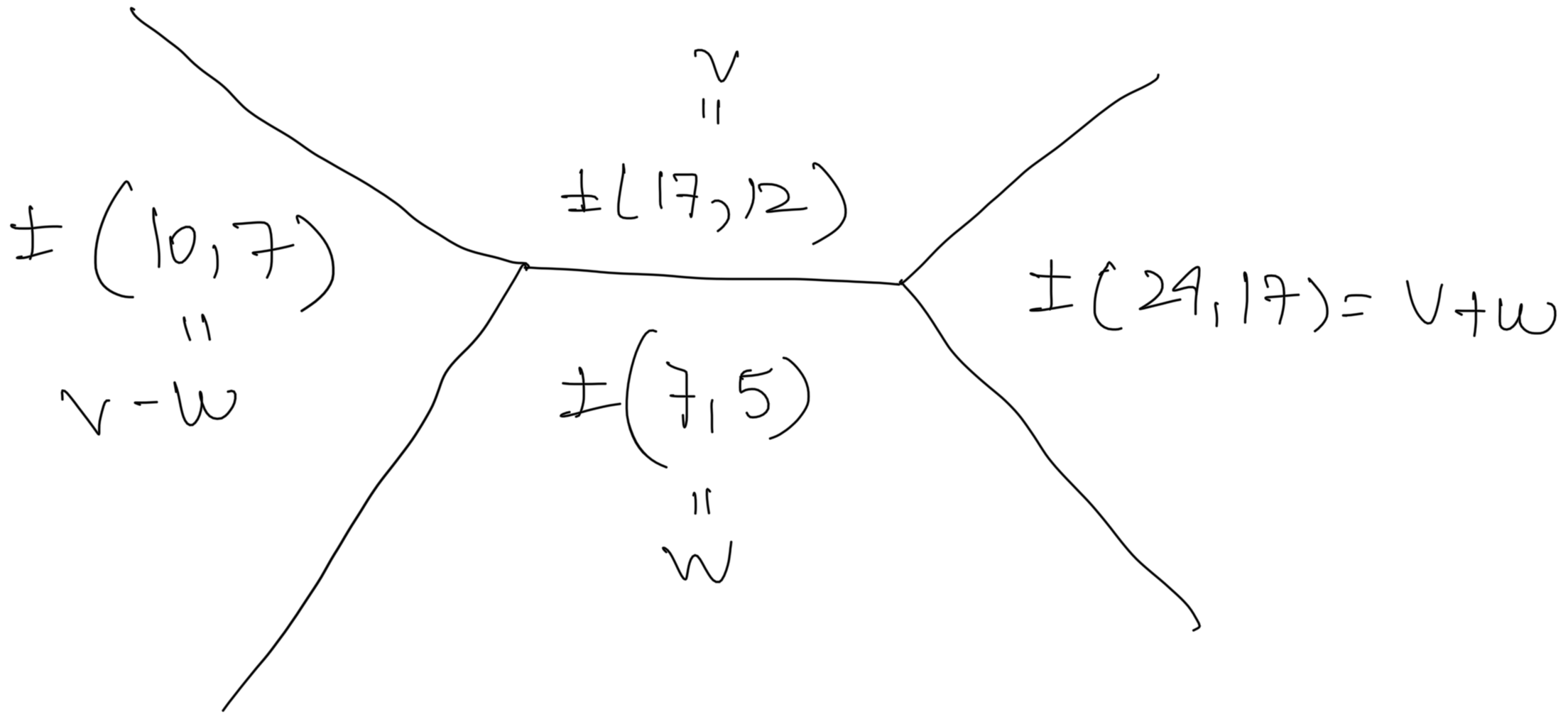
$\{v \pm w, w\}$ is a basis.

$$\begin{vmatrix} | & | \\ v & w \\ | & | \end{vmatrix} = \begin{pmatrix} | & | \\ v & v+w \\ | & | \end{pmatrix}$$

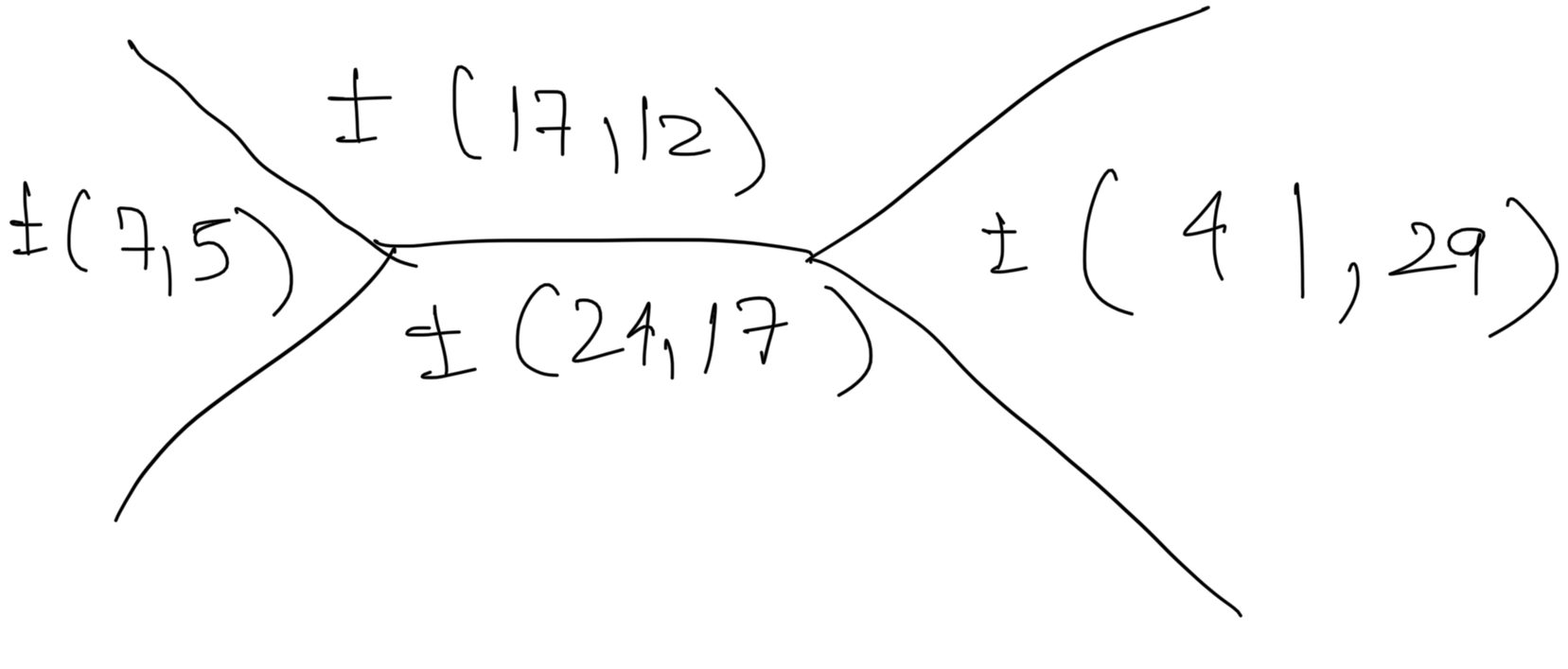
$$= \begin{vmatrix} | & | \\ v+w & w \\ | & | \end{vmatrix}$$

(Property of determinants)

Drawing domain topography near a vector



Let's extend this!



and so on !

$\{\pm(1,0), \pm(0,1)\}$ is called home basis.

Lemma: If $\{v, w\}$ is a basis, then by applying Euclidean Algorithm we get $\{\pm(1,0), \pm(0,1)\}$

Pf: Say $v = (a,b)$ $w = (c,d)$

$ad - bc = \pm 1$

Apply Euclidean algorithm on x-coordinates to get

a basis of the form $\{\pm(1,s), (0,t)\}$.

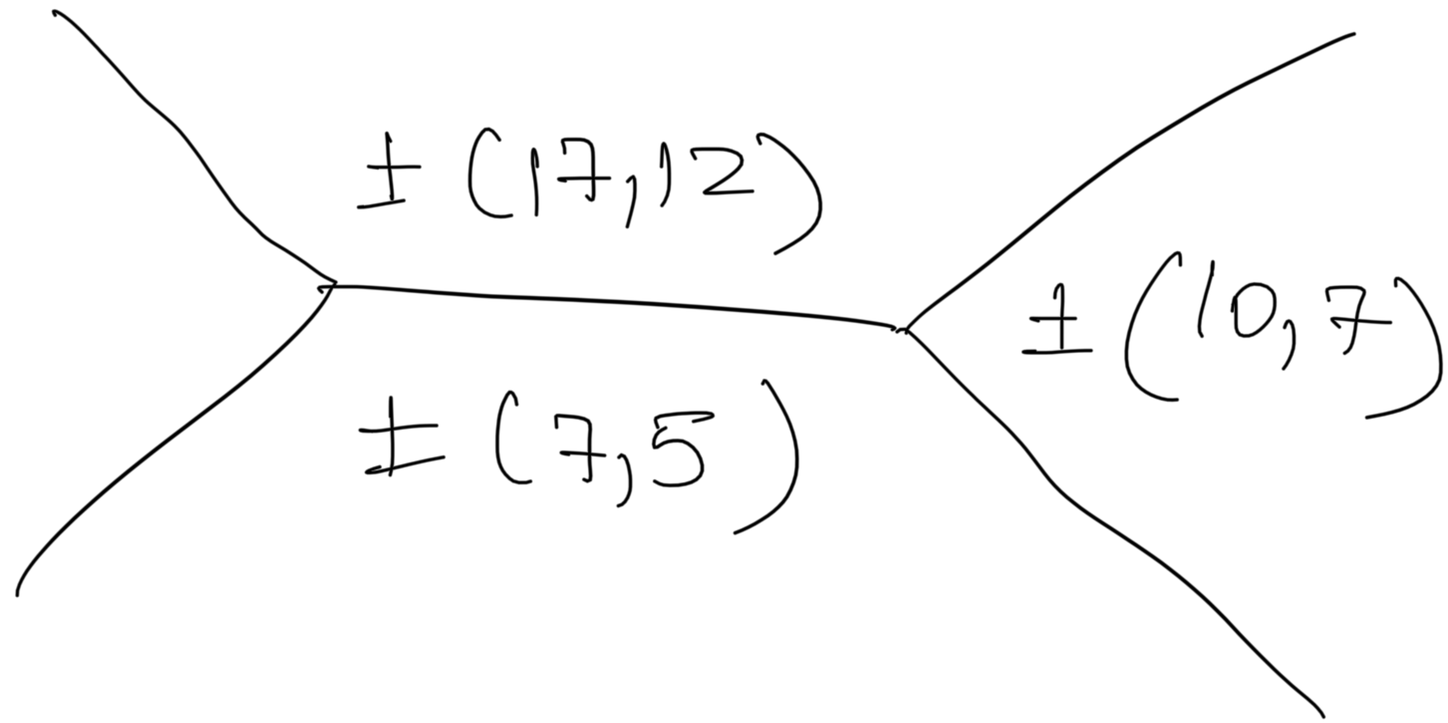
Each step of Euclidean algorithm looks like $v - qw$ so determinant is unchanged

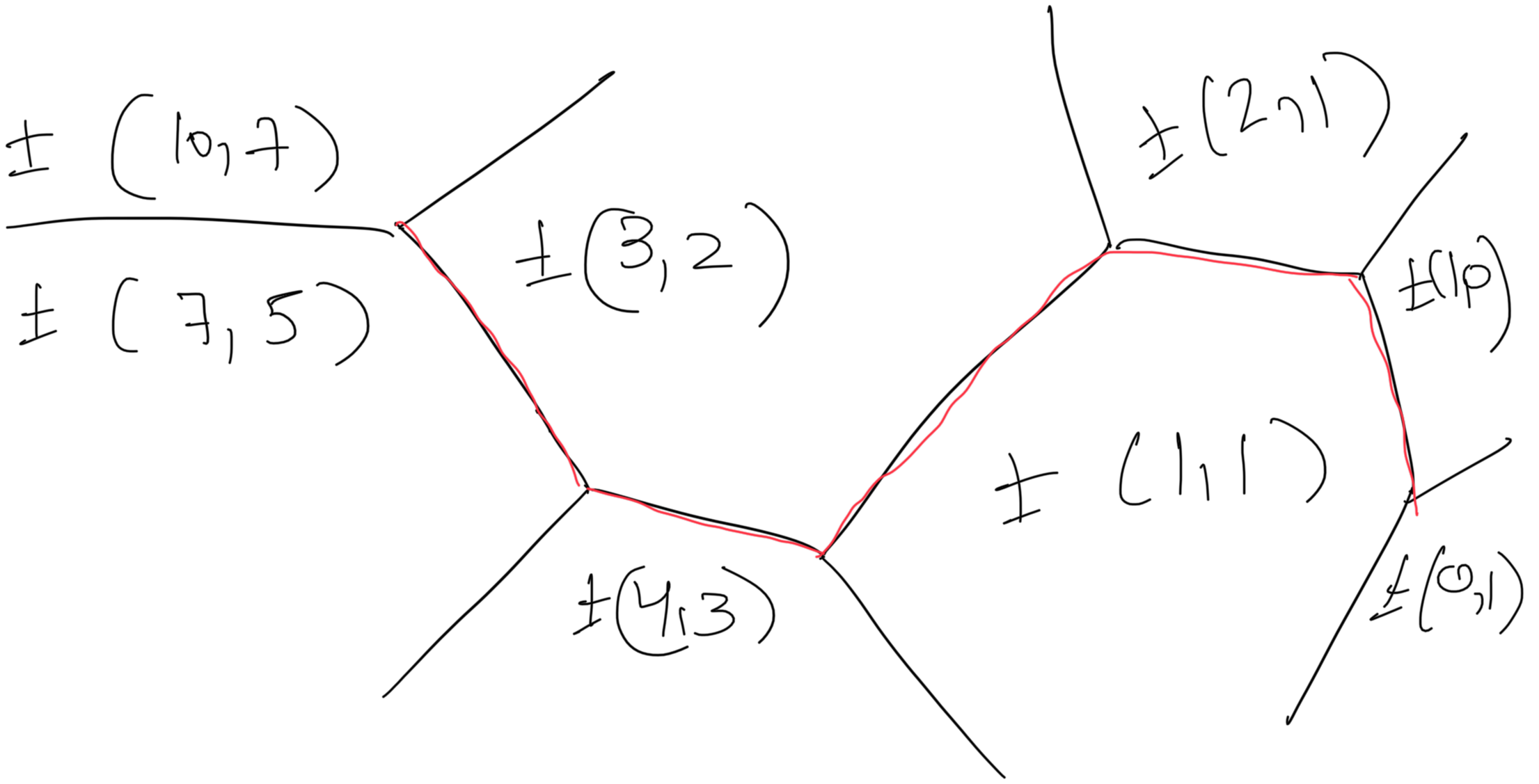
$$v = qw + w_1$$

$$\begin{vmatrix} 1 & 1 \\ v & w \end{vmatrix} = \pm \begin{vmatrix} 1 & 1 \\ w & v-qw \end{vmatrix}$$

$$\Rightarrow t = 1 \quad \boxed{(1,0) = (1,s) - s(0,1)}$$

Walk back home starting at




±(10,7)
±(7,5)
±(3,2)
±(4,3)
±(2,1)
±(1,1)
±(1,0)
±(0,1)