# Brian Conrad — Lecture 1

11/July/2011

notes by Manuel Araújo



## 1. Motivation

$x^2 + y^2 = z^2$ , $x, y, z \in \mathbb{Z}^+$ ( Without loss $\gcd(x,y,z) = 1$ ↪ primitive solution )

$(3,4,5)$ $(5,12,13)$

$(7,24,25)$ $(8,15,17)$ ...

Q: Are there infinitely many primitive solutions ?

Q: Parametric formula ?

Answer: $0 < m < n$ $\gcd(m,n) = 1$.

$\begin{cases} (n^2 - m^2, 2mn, n^2 + m^2), & n, m \text{ have opposite parity} \\ \left(\frac{n^2-m^2}{2}, mn, \frac{n^2+m^2}{2}\right), & n, m \text{ odd} \end{cases}$

Ex:

| $(m,n)$ | $(1,2)$ | $(1,3)$ | $(2,3)$ | $(2,5)$ |
|---|---|---|---|---|
| output | $(3,4,5)$ | $(4,3,5)$ | $(5,12,13)$ | $(21,20,29)$ |

- Where does this come from ?
- what about $3x^2 + 2y^2 = 5z^2$
  $7x^2 - 23y^2 = 15z^2$ ...

- Ex: $7x^2 - 23y^2 = 15z^2$ has no nonzero $\mathbb{Z}$-solution, for mod 3 reasons ( Exer I.4 (1) )

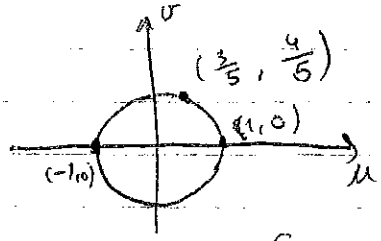
But $7x^2 + 23y^2 = 15z^2$ has solution $(4,1,3)$.

We'll see that the existence of a least one solution is number theory. If a solution exists, finding a parametric formula is geometry.

Rem: Once we have one solution, there is always a parametric formula giving all ( inf many) solutions

## 2. Geometric trick (idea):

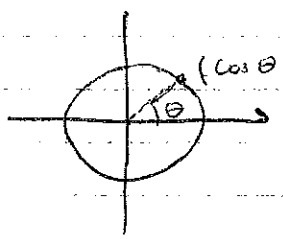
$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \quad \Leftrightarrow \quad \boxed{u^2 + v^2 = 1, \quad u, v \in \mathbb{Q}}$$




Points from pythagorean triples are in the first quadrant,

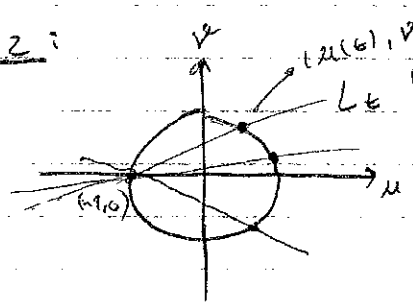
Can we understand $\mathbb{Q}$-points on the circle.

Trig:




$\leftarrow$ Useless for understanding $\mathbb{Q}$-points

Method 2:




Ex: $(u(1), v(1)) = (0, 1)$

Claim: $t$ is rational iff $u(t)$ and $v(t)$ is rational.

($\Leftarrow$): Easy.

($\Rightarrow$): Given $t \in \mathbb{Q}$, let's show that $L_t \cap C = \{(-1,0), \mathbb{Q}\text{ pt}\}$

What is $L_t$? Line of slope $t$ through $(-1, 0)$.

$$\frac{v-0}{u-(-1)} = t \quad \Leftrightarrow \quad v = t(u+1).$$

$$L_t \cap C = \{u^2 + t^2(u+1)^2 = 1\} = \{-1, (?)\}$$

The solutions are the $u$ coordinates of the intersection points.
The polynomial has rational coefficients and one of the roots is rational, therefore the other one is also rational $\longrightarrow$ $u(t)$ is rational.
But $v(t) = t(u(t)+1)$ therefore $v(t)$ is rational.

Let's compute $u(t)$ and $v(t)$.

Let $L$: $u^2 + t^2(u+1)^2 = 1$

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

$$\Leftrightarrow u^2 + \frac{2t^2}{1+t^2}u + \frac{t^2-1}{1+t^2} = 0 \qquad \Leftrightarrow (u+1)(u-u(t)) = 0$$

$$\Rightarrow -1 + u(t) = \frac{-2t^2}{1+t^2} \qquad \left(\sum \text{roots} = -a_{n-1}\right)$$

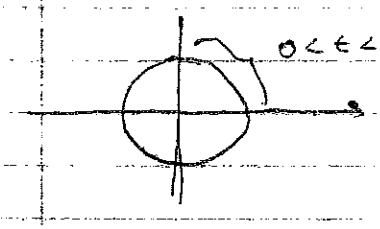
$$\therefore u(t) = \frac{1-t^2}{1+t^2} \qquad v(t) = \frac{2t}{1+t^2}$$

$$\downarrow$$

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

Remark: This works over any field (of char $\neq 2$)

Back to $\mathbb{Z}$: $t = \frac{m}{n}$ $\quad m, n \in \mathbb{Z}$ $\quad \gcd(m,n) = 1$



$0 < t < 1 \longrightarrow 0 < m < n$

$$\left(u\left(\frac{m}{n}\right), v\left(\frac{m}{n}\right)\right) = \left(\frac{1-\left(\frac{m}{n}\right)^2}{1+\left(\frac{m}{n}\right)^2}, \frac{2\left(\frac{m}{n}\right)}{1+\left(\frac{m}{n}\right)^2}\right)$$

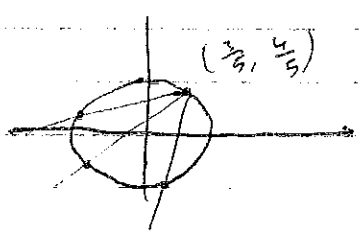
$$= \left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right) = \left(\frac{x}{z}, \frac{y}{z}\right)$$

$$\Rightarrow (x,y,z) = (n^2-m^2, 2mn, n^2+m^2) \quad \text{up to proportionality!}$$

Exercise: The only thing that can go wrong is a common factor of 2, when $m, n$ are odd.

## 3. Generalizations

- We can use any basepoint (over $\mathbb{Q}$)

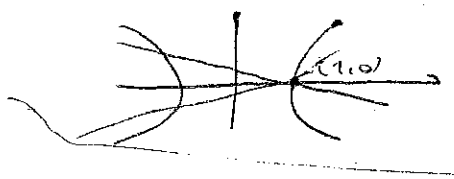


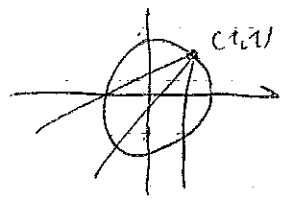

$$L_t = \left\{ \frac{v - \frac{4}{5}}{u - \frac{3}{5}} = t \right\} = \left\{ v = \frac{4}{5} + t\left(u - \frac{3}{5}\right) \right.$$

We can compute $L_6 \cap C$ : Exercise I.2

$x^2 - 7y^2 = z^2 \rightsquigarrow u^2 - 7v^2 = 1$

$3x^2 + 2y^2 = 5z^2 \rightsquigarrow 3u^2 - 2v^2 = 5$




$$\left( \frac{2t^2 - 4t - 3}{2t^2 + 3} \, , \, \frac{-2t^2 - 6t + 3}{2t^2 + 3} \right)$$

- The method works for any conic

$$a u^2 + b v^2 = c$$

We set a parametrization $(u(t), v(t))$ for the curve where $u(t), v(t)$ are rational functions in $t$ over $\mathbb{Q}$, provided we have one $\mathbb{Q}$-point.

Ex: $x^2 + y^2 = 3z^2 \longrightarrow u^2 + v^2 = 3$ has no $\mathbb{Q}$-points (Exercise)