Lecture I

B. Conrad

1. Motivation

$x^2+y^2=z^2$

$x,y,z \in \mathbb{Z}^+$

$\gcd(x,y,z)=1$ (primitive)

$(3,4,5)$

$(5,12,13)$

$(7,24,25)$

$(8,15,17)$

- are there infinitely many?
- there's a "parametric" formula?

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

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

(These solution are indeed primitive: Exercise 1)

Ex

(m,n)	$(1,2)$	$(1,3)$	$(2,3)$
output	$(3,4,5)$	$(4,3,5)$	$(5,12,13)$

- Where did this come from?
- What about $3x^2+2y^2=5z^2$? Here is solution?

  $7x^2+23y^2=15z^2$? Here is infinitely many?

For example: $7x^2-23y^2=15z^2$ has no non-zero integer solution

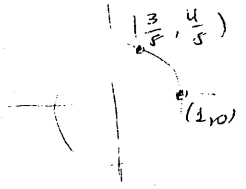
But $7x^2+23y^2 = 15z^2$ has solutions $(4,1,3)$

We'll see that the existence of at least one solution is number theory. But, if a solution exist, the parametric formula (creating solutions) is geometry.

Warn: Once have one solution, always a parametric formula giving all (infinitely many) solutions (for quadratic equations)

Geometric trick (idea)

~~We restrict~~ Consider $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \iff u^2+v^2=1$ with u, v rational.

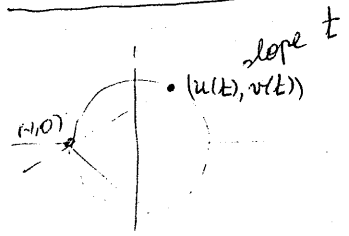


Pythagorean solutions in the first quadrant

so we understand "rational points" on the circle?

really, points on the circle are parametrized by angles $(\cos\theta, \sin\theta)$. But this parametrization is not useful to understand rationality of points.

Alternative method:



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

Claim: this parametrization is much better for our purpose because

$t \in \mathbb{Q} \iff (u(t), v(t)) \in \mathbb{Q} \times \mathbb{Q}$

(proof)

"$\Leftarrow$" easy

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

What is L_t $\quad \frac{v-0}{u-(-1)} = t \quad v = t(u+1)$

$L_t \cap C = \{u^2 + t^2(u+1)^2 = 1 \quad : v = t(u+1)\}$

~~quadratic equation in u~~ ~~solutions are u coordinates of these points~~.

But we know one of the solution is rational

Key: $\alpha, \beta, \gamma \in \mathbb{Q}$ $\quad \alpha x^2 + \beta x + \gamma = 0$

Σ roots $= -\beta/\alpha \in \mathbb{Q}$ | one root rational $\Rightarrow$ the other root ~~must be~~ rational.

$\therefore u(t) \in \mathbb{Q}$ when t is rational. (and $v(t) = t(u+1)$)

Note (1) It works because we are with quadratic equation! Not longer true in higher degrees.

Note (2) Same game can be play for any conic.

let's compute $(u(t), v(t))$

$L_t \cap C$ $\quad u^2 + t^2(u+1)^2 = 1$

$u^2 + t^2u^2 + t^2 2u + t^2 = 1$

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

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

We know that $u=-1$ is a solution.

$(u+1)(u - u(t)) = 0$

and we know $\quad -1 + u(t) = \frac{-2t^2}{1+t^2}$ (*)

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

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

Note: this parametrization works over any field $\mathrm{char} \neq 2$. (because (*))

Back to $\mathbb{Z}$.

$t = \frac{m}{n}$ $\quad m, n \in \mathbb{Z}$, $\gcd(m,n) = 1$ $\quad n \neq 0$

one gets the Pythagorean triangle.

$(u(\frac{m}{n}), v(\frac{m}{n})) = \left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right)$ { not true that it is primitive.

$(n^2-m^2, 2mn, n^2+m^2)$ solution up to primitive !!

3. Generalizations

- Can use any base point (over $\mathbb{Q}$).

For example, taking $(\frac{3}{5}, \frac{4}{5})$

one gets $L_t = \{ v = \frac{4}{5} + t(u - \frac{3}{5}) \}$

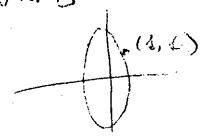
Exercise: compute $L_t \cap C$. (another parametrization) (harder identification of primitivity.)

- Can use for other quadratic equations.

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

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

$\rightsquigarrow \frac{3}{5}u^2 + \frac{2}{5}v^2 = 1$



using $(1,1)$ one gets

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

We see: for any conic $au^2 + bv^2 = c$ $\quad (a,b,c) \in \mathbb{Q}$-test we get a parametrization $(u(t), v(t))$ for the curve where $u(t), v(t)$ are rational functions over $\mathbb{Q}$, PROVIDED we have one $\mathbb{Q}$-point.

Ex $x^2 + y^2 = 3z^2 \rightsquigarrow u^2 + v^2 = 3$ has NOT $\mathbb{Q}$-points.