B. CONRAD class 1

11 de Julho de 2011

1 Motivation

Let's consider the equation $x^2 + y^2 = z^2$. We want to find solutions in $\mathbb{Z}^+$ such that $\gcd(x, y, z) = 1$ (primitive solutions). There are sereval questions that arise:

1. Are there infinitely many solutions?
2. Is there a parametric formula?

We are going to show that for this equation the answer to those questions is yes. The parametric formula for the solutions is $(n^2 - m^2, 2mn, n^2 + m^2)$ if n and m have opposite parity and $\frac{1}{2}(n^2 - m^2, 2mn, n^2 + m^2)$ otherwise. In any case we require $0 < m < n$ and $\gcd(m, n) = 1$.

1. Where did this come from?
2. What about other equations, like $3x^2 + 2y^2 = 5z^2$?

For instance, $7x^2 - 23y^2 = 15z^2$ has no integer solutions (this can be show using $\mod 3$ reasoning). On the other hand, we'll see that the existance of at least one solution guarantees that there are infinitely many other and that a parametric formula for generating them all can be found. The problema of cheking if a solution exists is a problem in Number Theory and that, on the other hand, finding the parametric formula is a Geometric problem.

2 Generic Trick

Since $z \neq 0$, $x^2 + y^2 = z^2 \Leftrightarrow \frac{x}{z}^2 + \frac{y}{z}^2 = 1$. This way we get an equation of the form $u^2 + v^2 = 1$ where $u, v \in \mathbb{Q}$. Can we understand Q-points on a cicle? The trigonometric parametrization is useless for understanding rational points. Instead we will use another method:

1. We fix a Q-point p in the unit circle C (here we will use $p = (-1, 0)$.

2. Then, for each $t \in \mathbb{Q}$ let L_t be the line that goes through $p = (-1, 0)$ and has slope t.

3. Let $(u(t), v(t))$ be the other point of intersection of C and L_t.

Claim: $t \in Q \Leftrightarrow (u(t), v(t)) \in \mathbb{Q}^2$

Proof:
($\Leftarrow$) Trivial. Just think about the slope of a line that goes through two rational points.
($\Rightarrow$) Given $t \in \mathbb{Q}$, L_t has equation $\frac{v-0}{u-(-1)} = t \Leftrightarrow v = t(u+1)$. To be in C we must have $u^2 + t^2(u+1)^2 = 1$ wich is a polynomial in u of degree 2.
We know that -1 is a root. The sum of the roots of a polynomial of degree n must be minus the coeficient of x^{n-1}. Since the polynomial is in $Q[u]$, the other root must be rational. Then $u(t) \in \mathbb{Q}$ and so $v(t) = t(u(t)+1) \in \mathbb{Q}$. This ends the proof.

By straightforward calculations we can find the explicit formulas

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

Note that this works in any field K (maybe not $c(K) = 2$). Now, putting $t = \frac{m}{n}$ with $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$ we find that

$$u(\tfrac{m}{n}) = \frac{1-\frac{m}{n}^2}{1+\frac{m}{n}^2} = \frac{n^2-m^2}{n^2+m^2}, \quad v(t) = \frac{2\frac{m}{n}}{1+\frac{m}{n}^2} = \frac{2mn}{n^2+m^2}$$

This way we get te formula from before $(x, y, z) = (n^2 - m^2, 2mn, n^2 + m^2)$ up to a common factor ($n^2 - m^2$ and $2mn$ may not be coprime).

3 Generalizations

We can use any base point (over $\mathbb{Q}$). The only reason that we used $p = (-1, 0)$ was to get simple algebraic expressions. Also this method will work for any conic $au^2 + bv^2 = c$ provided we have a rational point on the curve.