Pythagorean triples and Hilbert's Theorem 90

Noam D. Elkies

The classical parametrization of Pythagorean triples is well known:

Theorem. *Integers x, y, z satisfy the Diophantine equation $x^2 + y^2 = z^2$ if and only (x, y, z) is proportional to $(m^2 - n^2, 2mn, m^2 + n^2)$ for some integers m, n.*

This is usually proved either arithmetically, by rearranging the equation as $z^2 - y^2 = x^2$ and factoring both sides, or geometrically, by the usual procedure for parametrizing a plane conic. It seems not to have been recognized that this parametrization of Pythagorean triples is equivalent to a special case of Hilbert's Theorem 90.

Proof: We may assume that $z \neq 0$, because if $z = 0$ then $x = y = 0$ and we may take $(m, n) = (0, 0)$. Let w, then, be the complex number $(x + iy)/z$ in the quadratic extension $\mathbf{Q}(i)$ of $\mathbf{Q}$. The norm of w equals $(x^2 + y^2)/z^2 = 1$. Thus by Hilbert there exists $a \in (\mathbf{Q}(i))^*$ such that $w = a/\overline{a}$. For any nonzero $r \in \mathbf{Z}$ we have $ar/\overline{ar} = a/\overline{a}$. There exists nonzero $r \in \mathbf{Z}$ such that $ar \in \mathbf{Z}[i]$, say $ar = m + in$ with $m, n \in \mathbf{Z}$, not both zero. We then calculate

$$\frac{x + iy}{z} = w = ar/\overline{ar} = \frac{m + in}{m - in} = \frac{(m + in)^2}{(m + in)(m - in)} = \frac{(m^2 - n^2) + i(2mn)}{m^2 + n^2},$$

which is to say that (x, y, z) is proportional to $(m^2 - n^2, 2mn, m^2 + n^2)$, as claimed.

Generalizations. In the same way we can parametrize the solutions of the Diophantine equation $x^2 + Axy + By^2 = z^2$ for any constants A, B such that the discriminant $A^2 - 4B$ is not a square. Again we may assume that $z \neq 0$. Instead of $\mathbf{Q}(i)$ we work in the quadratic extension $\mathbf{Q}(r)$ of $\mathbf{Q}$, where r is a solution of $r^2 - Ar + B = 0$. Then $x^2 + Axy + By^2$ is the norm of $x + ry$, so $x^2 + Axy + By^2 = z^2$ if and only if $w := (x + ry)/z$ has norm 1. Thus again $w = a/\overline{a}$ for some $a \in (\mathbf{Q}(r))^*$, where $\overline{a}$ denotes the algebraic conjugate of a. Hence

$$\frac{x + iy}{z} = w = \frac{m + rn}{m + \overline{r}n} = \frac{m + rn}{m + (A - r)n} = \frac{(m + rn)^2}{m^2 + Amn + Bn^2}$$

for some integers m, n, not both zero. We conclude that (x, y, z) is proportional to $(m^2 - Bn^2,\ 2mn + An^2,\ m^2 + Amn + Bn^2)$.

More generally yet, we may consider $x^2 + Axy + By^2 = Cz^2$ for some nonzero constant C, with A, B as before. We then want $w = (x+ry)/z \in \mathbf{Q}(c)$ with norm $w\overline{w} = C$. In general such w need not exist. But if we know one solution (x_0, y_0) of $x^2 + Axy + By^2 = Cz^2$ with $z_0 \neq 0$, then we know $w_0 = (x_0 + ry_0)/z_0 \in \mathbf{Q}(c)$ such that $w_0\overline{w}_0 = C$. Then $w\overline{w} = C$ if and only if w/w_0 has norm 1, so $w = aw_0/\overline{a}$ and we can proceed as before.