Parabola Volume 59, Issue 2 (2023)

90 provides the right angle of approach

B. Sury[1]

1 Introduction

Arguably, when we hear the number 90 mentioned, it is very likely that the first thought that may come to mind is that of a right angle. Perhaps, the next thing which comes to the mind is Pythagoras' Theorem. A natural topic of discussion then is to find the Pythagorean triplets of positive integers (a, b, c) so that $a^2 + b^2 = c^2$. When we try to characterize such integer triplets, the equation we solve is $x^2 + y^2 = 1$ for solutions in rational numbers x, y. So, we are looking at a 'rational point' (x, y) on the unit circle. Here, a novel method (or at least a method that is perhaps not well known among high school or beginning college students) is to view any point on the unit circle as a complex number $e^{i\theta}$ and write

$$e^{i\theta} = \frac{e^{i\theta/2}}{e^{-i\theta/2}} \, .$$

This somewhat strange rephrasing is a special case of something that goes by the name of Hilbert's Theorem 90. Without going to a general discussion of Hilbert's Theorem 90, we discuss special cases which are completely elementary.

The purpose of our note is to use this point of view to not only recover the well-known parametrisation of the sides of all integer-sided right-angled triangles but also to completely parametrise the lengths of the sides of all integer-sided triangles with an angle having a rational cosine value. So, one may say that Hilbert's Theorem 90 gives the right angle of approach to this problem!

Our discussion below yields some interesting tidbits. For instance, the integer-sided triangles with an angle having cosine value $1/10$ are precisely the triangles with sides that are multiples of $(21, 200, 199)$. We also mention how certain types of Diophantine equations can be naturally dealt with by the same method.

Right-angled triangles or those with an angle of 60 or 120 degrees have been discussed in several places - too numerous to mention. A few of the comparatively accessible references are [1, 2, 3, 4, 5] and some mathematical blogs. Nevertheless, we hope that our discussion is elementary, self-contained and, hopefully, is different and has some novel features. Furthermore, the name 'Hilbert's Theorem 90' may sound grandiose, but it is a statement with a completely elementary one-line proof in the context that we discuss.

[1] B. Sury is a Professor of Mathematics at the Indian Statistical Institute in Bangalore, India.

2 Hilbert's Theorem 90 - Baby Version

If $\triangle ABC$ is a right-angled triangle with positive integer sides a, b, c, then Pythagoras' Theorem states that $a^2 + b^2 = c^2$. If $x = a/c$ and $y = b/c$, then these are rational numbers satisfying $x^2 + y^2 = 1$. In terms of the complex number $x + iy$, this is saying that $|x + iy|^2 = 1$. If we think of $x + iy$ as $e^{i\theta}$ for some θ, then the equality

$$e^{i\theta} = \frac{e^{i\theta/2}}{e^{-i\theta/2}}$$

actually gives us

$$x + iy = \frac{u + iv}{u - iv}$$

for some *rational numbers* u, v. By clearing denominators, we may assume that u, v are integers which are relatively prime. Then, the right-hand side above becomes

$$\frac{(u + iv)^2}{u^2 + v^2} = \frac{u^2 - v^2}{u^2 + v^2} + i\frac{2uv}{u^2 + v^2}\,.$$

On equating the real and imaginary parts, we have

$$x = \frac{a}{c} = \frac{u^2 - v^2}{u^2 + v^2} \quad \text{and} \quad y = \frac{b}{c} = \frac{2uv}{u^2 + v^2}\,.$$

From this, it is easy to deduce that any *primitive* Pythagorean triple (that is, when a, b, c are pairwise relatively prime) is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$.

More generally, consider any triangle $\triangle ABC$ whose sides are integers a, b, c with the usual convention of naming. One has the cosine law

$$c^2 = a^2 + b^2 - 2ab \cos \angle C\,.$$

We will show that an analogous characterization exists when $\cos \angle C = p/q$, a rational number. Note that p/q could be 0 or have any sign. We assume that when $\cos \angle C = \frac{p}{q} \neq 0$, then $\frac{p}{q}$ is in reduced form and $q > 0$. For consistency of notation, we take $q = 1$ when $p = 0$. Then, we have

$$x^2 + y^2 - 2\,\frac{p}{q}xy = 1$$

where $x = a/c$ and $y = b/c$. The quadratic polynomial on the left is naturally factorized into two linear polynomials (at least over the complex numbers) as

$$x^2 + y^2 - 2\frac{p}{q}xy = \left(x - \frac{p - \sqrt{p^2 - q^2}}{q}y\right)\left(x - \frac{p + \sqrt{p^2 - q^2}}{q}y\right).$$

The right hand side above is a kind of measure of the size (known as the norm) of the number $x - \frac{p-\sqrt{p^2-q^2}}{q}y$. Observe that when $\angle C$ is a right angle, the factorization is the familiar

$$x^2 + y^2 = (x + iy)(x - iy)$$

and the 'norm' of $x+iy$ is x^2+y^2. Further, we notice that being the cosine of an angle of a triangle, $|p/q| < 1$ which means that $\sqrt{p^2-q^2}$ is a purely imaginary complex number.

We discuss Hilbert's Theorem 90 in our set-up. Consider any square-free integer $d \neq 0, 1, -1$ (of any sign). Let $x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ have 'norm' 1 as mentioned above; that is, $(x+\sqrt{d}y)(x-\sqrt{d}y) = x^2 - dy^2 = 1$. Hilbert's Theorem 90 in this context simply asserts the following.

Lemma 1. *(Hilbert's Theorem* 90 *for 'quadratics') There exist* $u, v \in \mathbb{Q}$ *so that*

$$x + y\sqrt{d} = \frac{u + v\sqrt{d}}{u - v\sqrt{d}}.$$

Proof. We observe now that this indeed has a one-line proof. The proof is obtained by simply solving the following for u, v:

$$x + y\sqrt{d} = \frac{x + 1 + y\sqrt{d}}{x + 1 - y\sqrt{d}}$$

when $x^2 - dy^2 = 1$. □

3 Parametrizing integer-sided triangles with rational cosine of angle

Returning to our triangles $\triangle ABC$ with $\cos\angle C = \frac{p}{q}$, we have $x^2 + y^2 - 2\frac{p}{q}xy = 1$ where $x = a/c$ and $y = b/c$. Thus, Hilbert's Theorem 90 above gives us

$$x - \frac{p - \sqrt{p^2-q^2}}{q}y = \frac{u + v\sqrt{p^2-q^2}}{u - v\sqrt{p^2-q^2}}$$

where we can assume, by clearing denominators, that u, v are relatively prime integers. Further, we may assume that $v > 0$ (at the moment u could have any sign). The right-hand side above can be rewritten as follows:

$$\frac{u + v\sqrt{p^2-q^2}}{u - v\sqrt{p^2-q^2}} = \frac{(u + v\sqrt{p^2-q^2})^2}{u^2 - v^2(p^2-q^2)} = \frac{u^2 + v^2(p^2-q^2) + 2uv\sqrt{p^2-q^2}}{u^2 - v^2(p^2-q^2)}.$$

Therefore, we obtain

$$\frac{a}{c} - \frac{p - \sqrt{p^2-q^2}}{q}\frac{b}{c} = \frac{u^2 + v^2(p^2-q^2) + 2uv\sqrt{p^2-q^2}}{u^2 - v^2(p^2-q^2)}.$$

Equating the real and imaginary parts, we have

$$\frac{aq - bp}{cq} = \frac{u^2 + (p^2-q^2)v^2}{u^2 - (p^2-q^2)v^2};$$

therefore,

$$\frac{b}{cq} = \frac{2uv}{u^2 - (p^2 - q^2)v^2} \, .$$

Note that $\cos \angle C = p/q$ means $q^2 > p^2$. We have fixed notation so that $q > 0$ (p may have any sign) and $v > 0$ in the parametrization. Also, for the special case $\cos(C) = 0$, we take $p = 0$ and $q = 1$ for convenience. So, we have now obtained the following result.

Proposition 2. *If $\triangle ABC$ is a triangle with integer sides a, b, c and $\cos \angle C = \frac{p}{q}$ with $q > 0$, then there exist relatively prime integers u, v with $v > 0$ so that*

$$(a : b : c) = (u^2 - (q^2 - p^2)v^2 + 2puv : 2quv : u^2 + (q^2 - p^2)v^2) \, .$$

Further, the right-hand side give the side lengths of a triangle when $u > (q - p)v$.

The last statement is simply a consequence of the constraint that the sum of two sides is larger than the third one and the fact that the side-lengths are positive. Finally, we also point out that $\angle C$ need not be the largest angle, as we can see in many examples below.

4 Examples

Example 1. If $\angle C = 90°$, then note that $p = 0, q = 1$ which gives the parametrization

$$(u^2 - v^2 : 2uv : u^2 + v^2)$$

with $u > v > 0$ for the sides of any integer-sided right-angled triangle.

Example 2. If $\angle C = 60°$, then note that $p = 1, q = 2$ which gives the parametrization

$$(u^2 - 3v^2 + 2uv : 4uv : u^2 + 3v^2)$$

with $u > v > 0$. For instance, we have the following special cases:

$(u, v) = (2, 1)$ gives a triangle with sides $(5, 8, 7)$;
$(u, v) = (3, 1)$ gives sides proportional to $(12, 12, 12)$ - i.e., equilateral triangles;
$(u, v) = (3, 2)$ gives sides proportional to $(9, 24, 21)$ - i.e., multiples of $(3, 8, 7)$;
$(u, v) = (4, 1)$ gives sides that are multiples of $(21, 16, 19)$;
$(u, v) = (4, 3)$ gives sides that are multiples of $(13, 48, 43)$;
$(u, v) = (5, 1)$ gives sides proportional to $(32, 20, 28)$ - i.e., multiples of $(8, 5, 7)$;
$(u, v) = (5, 2)$ gives sides that are multiples of $(33, 40, 37)$;
$(u, v) = (5, 3)$ gives sides proportional to $(28, 60, 52)$ - i.e., multiples of $(7, 15, 13)$;
$(u, v) = (5, 4)$ gives sides that are multiples of $(17, 80, 73)$.

By the examples $(u, v) = (2, 1), (5, 1)$, note that different values of u, v can give the same triangle. Note also that a right-angled triangle with one angle of 60 degrees cannot occur here, as such a triangle is not integer-sided.

Example 3. If $\angle C = 120°$, then note that $p = -1, q = 2$ which gives the parametrization

$$(u^2 - 3v^2 - 2uv : 4uv : u^2 + 3v^2)$$

with $u > 3v$. For instance, we have the following special cases:

$(u, v) = (4, 1)$ gives sides that are multiples of $(5, 16, 19)$;
$(u, v) = (5, 1)$ gives sides proportional to $(12, 20, 28)$ - i.e., multiples of $(3, 5, 7)$;
$(u, v) = (7, 2)$ gives sides that are multiples of $(9, 56, 61)$.

Example 4. If $\cos\angle C = 17/24$, then we get the parametrization

$$(u^2 - 7v^2 + 34uv : 48uv : u^2 + 7v^2)$$

with $u > 7v$. For instance,

$(u, v) = (8, 1)$ gives triangle sides that are multiples of $(329, 384, 71)$.

Example 5. In general, let $\cos\angle C = p/q \in (0, 1)$, and consider the parametrization

$$(u^2 - (q^2 - p^2)v^2 + 2puv, 2quv, u^2 + (q^2 - p^2)v^2$$

where $u > (q - p)v$. Take $(u, v) = (q - p + 1, 1)$; we then obtain triangles with sides proportional to

$$(2q + 1, 2q(q - p + 1), 2(q + 1)(q - p) + 1)\,.$$

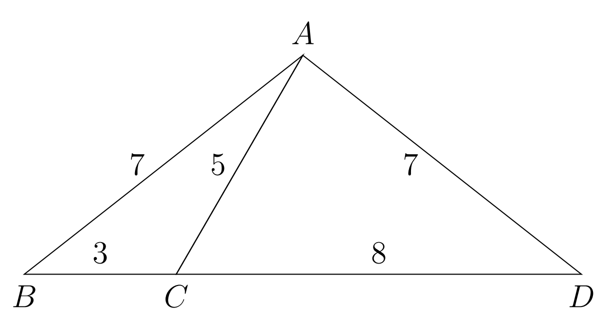
In particular, if $p = 1$; i.e., if $\cos\angle C = 1/q$ and $u = q+1$ and $v = 1$, then we get triangles with side lengths which are multiples of

$$(2q + 1, 2q^2, 2q^2 - 1)\,.$$

Just for fun, note that any integer-sided triangle with one angle, say C, such that $\cos\angle C = 1/10$ must have sides that are multiples of

$$(21, 200, 199)\,.$$

Example 6. Here is a special integer-sided triangle formed as a union of two triangles $\triangle ABC$ and $\triangle ACD$ with integer sides and $\angle ACD = 60°$.



5 Some Diophantine Equations

In the preceding discussions, one could say that Hilbert's Theorem 90 gives the right angle of approach to this parametrization problem. We dealt with Diophantine equations of the form $a^2 - db^2 = c^2$ for fixed square-free integers d using Hilbert's Theorem 90. Building on this theme, it is clear that we may consider more general Diophantine equations. In fact, if $\zeta = e^{2i\pi/p}$ for an odd prime number p, then the corresponding version of Hilbert's Theorem 90 is as follows. First, we recall that the smallest-degree polynomial $\Phi_p(x)$ with integer coefficients, and top coefficient 1, of which ζ is a root, is given by

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1\,.$$

For any complex number $z = \sum_{r=0}^{p-2} c_r \zeta^r$ with $c_i \in \mathbb{Z}$, one has the 'norm' defined as

$$N(z) = \prod_{k=1}^{p-1} \sum_{r=0}^{p-2} c_r \zeta^{kr}\,.$$

Then Hilbert's Theorem 90 in this situation is the following statement:

If $N(\sum_{r=0}^{p-2} c_r \zeta^r) = 1$, then there exist integers a_r ($0 \le r < p-1$) such that

$$\sum_{r=0}^{p-2} c_r \zeta^r = \frac{\sum_{r=0}^{p-2} a_r \zeta^r}{\sum_{r=0}^{p-2} a_r \zeta^{kr}}$$

where k is a 'primitive root' modulo p; that is, k has order $p-1$ modulo p.

Note that when $p = 3$, this is the norm above, $N(c_0 + c_1 e^{2i\pi/3}) = c_0^2 - c_0 c_1 + c_1^2$, and Hilbert's Theorem 90 is the statement that we have used earlier. Note that 2 is a primitive root modulo 3.

In passing, we mention that this example generalizes to certain complex numbers which generate what is called a Galois extension of $\mathbb{Q}$ with its Galois group being cyclic; we have a version of Hilbert's Theorem 90 and it allows us to deal with homogeneous polynomial equations of the form $\text{Norm}(x) = 1$. In principle, Hilbert's Theorem 90 shows that any such x is expressible as $y/\sigma(y)$ where σ is a so-called generator of the Galois group.

Recently, I learnt about an article (see [2]) by Shin-Ichi Katayama where the author considers numbers involving a primitive 7-th root of unity; the norm equation is a cubic homogeneous equation whose solutions are parametrized by Hilbert's Theorem 90. Readers are referred to some references mentioned in Katayama's paper which discuss Pythagorean triples using Hilbert's Theorem 90.

Let us look at one final example.

Example 7. Consider the discussion above for the case $p = 5$. Let $\zeta = e^{2i\pi/5}$ and note that 2 is a primitive root modulo 5 (the powers $2^1, 2^2, 2^3, 2^4$ of 2 modulo 5 are $2, 4, 3, 1$, respectively). Note that since $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$, we have

$$\zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3 .$$

Consider any number

$$x = a + b\zeta + c\zeta^2 + d\zeta^3$$

such that $\mathrm{Norm}(x) = 1$. Using $\zeta^5 = 1$ and simplifying etc., the expression for the norm is

$$(a + b\zeta + c\zeta^2 + d\zeta^3)(a + b\zeta^2 + c\zeta^4 + d\zeta)(a + b\zeta^4 + c\zeta^3 + d\zeta^2)(a + b\zeta^3 + c\zeta + d\zeta^4) .$$

This is a homogeneous polynomial $f(a, b, c, d)$ of degree 4 in a, b, c, d which vary in $\mathbb{Q}$. The equation $\mathrm{Norm}(x) = 1$ has solutions $x = \frac{p+q\zeta+r\zeta^2+s\zeta^3}{p+q\zeta^2+r\zeta^4+s\zeta}$ where we may assume that p, q, r, s are integers without a common factor greater than 1. The equation $\mathrm{Norm}(x) = 1$ gives a Diophantine equation of the form

$$f(a, b, c, d) = r^4$$

for integers a, b, c, d; hence, Hilbert's Theorem 90 would give a parametrization of all integer solutions. Indeed,

$$f(a, b, c, d) = (a+b\zeta+c\zeta^2+d\zeta^3)(a+b\zeta^2+c\zeta^4+d\zeta)(a+b\zeta^4+c\zeta^3+d\zeta^2)(a+b\zeta^3+c\zeta+d\zeta^4) .$$

Therefore, when $\mathrm{Norm}(x) = 1$, Hilbert's Theorem 90 gives $x = \frac{s+t\zeta+u\zeta^2+v\zeta^3}{s+t\zeta^2+u\zeta^4+v\zeta}$ where we may assume without loss of generality that s, t, u, v are integers without a common factor. Thus, one can multiply both the numerator and denominator above by the "conjugates" of the denominator and simplify to get an expression of the form $\frac{k+\ell\zeta+m\zeta^2+n\zeta^3}{w}$ where $w = \mathrm{Norm}(s + t\zeta^2 + u\zeta^4 + v\zeta) \in \mathbb{Z}$ and k, ℓ, m, n are polynomial expressions in s, t, u, v. By comparing the coefficients of $1, \zeta, \zeta^2, \zeta^3$, we get the ratios $(a : b : c : d)$ in terms of arbitrary integers s, t, u, v. Even though we obtain a parametrization of all the integer solutions of $f(a, b, c, d) = r^4$, the fourth-degree homogeneous polynomial $f(a, b, c, d)$ itself is not of any particular interest. Off-hand, there is no reason to think of studying such a complicated fourth-degree homogeneous polynomial. Suffice it to say that Hilbert's Theorem 90 gives solutions of many Diophantine equations that we may not even think of solving!

References

[1] N.D. Elkies, Pythagorean triples and Hilbert's Theorem 90, http://www.math.harvard.edu/~elkies/Misc/hilbert.pdf, last accessed on 2023-08-05.

[2] Shin-Ichi Katayama, Diophantine Equations and Hilbert's Theorem 90, *J. Math. Univ. Tokushima* **48** (2014), 35–40.

[3] T. Ono, *Variations on the Theme of Euler: Quadratic Forms, Elliptic Curves and Hopf Maps*, Plenum Press, 1994.

[4] E. Read, On integer-sided triangles containing angles of 120° or 60°, *The Mathematical Gazette* **90** (2006), 299–305.

[5] O. Taussky, Sums of squares, *Amer. Math. Monthly* **77** (1970), 805–830.

Address for Correspondence:
Indian Statistical Institute, 8th Mile Mysore Road
Bangalore 560059, India.
email: surybang@gmail.com