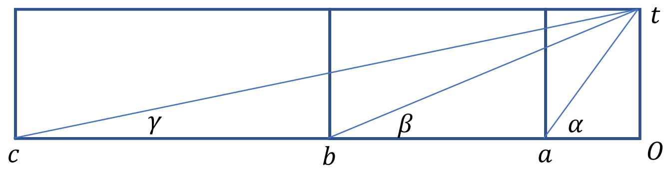
In TIP 14 we promised an explanation for our procedure for generating what we called *Gardner triples*. These were numbers notated $(a, b, c)_t$ arising from the following diagram, in which the angles satisfy $\alpha = \beta + \gamma$ and the lengths a, b, c and t are integer.



To form a connection between the angles and the lengths, we write $\gamma = \alpha - \beta$, then $\tan\gamma = \frac{\tan\alpha - \tan\beta}{1+\tan\alpha\tan\beta}$. Thus, $\frac{t}{c} = \frac{\frac{t}{a}-\frac{t}{b}}{1+\frac{t^2}{ab}}$, which on being rearranged gives $c = \frac{ab+t^2}{b-a}$.

For c to be an integer, we require the difference $b - a = D$ to be a factor of the numerator $ab + t^2$. We eliminate b from the expression for c and write $c = a + \frac{a^2+t^2}{D}$ showing that D must divide a sum of two squares.

It is now possible to see why the procedure given in TIP 14 works. If $a^2 + t^2$ is expressed as a product mn, we can let $D = m$, with $m \le n$, so that, on expanding the Gardner triple notation $(a, b, c)_t$, we write $(a, a+m, a+n)_t$. While this explains the procedure, we must look further to understand what constraints on the divisor D are required to ensure that the Gardner triple definition is satisfied.

We conjectured that a Gardner triple exists if and only if the difference $b - a$ is 1, or a prime of the form of the form $4k + 1$, or a product of such primes, or twice any of these quantities. The verification of the conjecture takes us well beyond secondary school mathematics.

To begin, we assume that a, b, c and t have no common factors since if they do the factors can be cancelled and the problem is merely rescaled. Note that if exactly one of a and t is even, then $a^2 + t^2$ has the form $4k + 1$. If both are odd, then $a^2 + t^2$ has the form $2(2k + 1)$. Clearly, D can contain the factor 2 at most once, which is consistent with the conjecture.

To proceed, we used results discovered by Diophantus, Euler, Fermat, Lagrange, Gauss and Dedekind. Briefly, these included:

- A product of two sums of two squares is also a sum of two squares. (Diophantus)
- If a number that is the sum of two squares is divisible by a prime that is the sum of two squares, then the quotient can be expressed as a sum of two squares. (Euler)
- A number that is not expressible as the sum of two squares cannot divide a sum of two squares. (Euler)
- If $p = 4k + 1$ is prime, then there exists an integer m such that p divides $m^2 + 1$. (Lagrange, using Fermat's *little* theorem)
- Every $4k + 1$ prime is expressible as the sum of two squares. (Dedekind, using Gaussian integers, $m^2 + 1 = (m + i)(m - i)$. Also proved by Euler by another method.)

Challenge 15: Fill in the gaps.