Pythagorean triples, or the design of a theorem

This note is a byproduct of looking at

(0) $$(x+y)^2 = (x-y)^2 + 4xy$$,

which was used in EWD1171 to show that the geometric mean is at most the arithmetic mean.

We are interested in Pythagorean triples, i.e. triples (a,b,c) of positive integers such that

(1) $$c^2 = a^2 + b^2$$,

$(3,4,5)$ being an example known since Antiquity. Just searching for another example we'll find sooner or later $(5,12,13)$, $(15,8,17)$, and perhaps even more, but searching is a painful process, and this raises the question whether this pain can be avoided by generating Pythagorean triples much more efficiently.

The answer is "Yes", and formula (0) is the stepping stone: it expresses a square as the sum of two squares, provided xy is a square! We can restrict ourselves to pairs x,y that are relatively prime, for a common factor of x and y is shared by $a, b, \& c$ and can be divided out. (For instance, with $x,y := 12,3$, (0) yields

$$225 = 81 + 144$$

but the triple $(9,12,15)$ is not a great discovery when the smaller Pythagorean triple $(3,4,5)$ is already known.) From

$(x \underline{\text{gcd}}\ y = 1)$ and $(xy$ is a square$)$

we conclude that x and y themselves are squares. Substituting $x,y := p^2, q^2$ into (0) yields

$$(p^2+q^2)^2 = (p^2-q^2)^2 + (2\cdot p\cdot q)^2$$

and hence (a,b,c), given by

(2) $\quad a = p^2 - q^2$
$\quad\quad b = 2\cdot p\cdot q$
$\quad\quad c = p^2 + q^2$

is a Pythagorean triple. We can restrict ourselves to pairs p,q such that

(3a) $\quad p > q$
(3b) $\quad p \underline{\text{gcd}}\ q = 1$
(3c) $\quad \text{odd}.(p+q)$.

Constraint (3c) has been introduced because $\text{even}.(p+q)$ leads to a triple (a,b,c) with a common factor of 2 .

We have achieved a lot: from (2) and (3) one can deduce that the number of Pythagorean triples whose elements are relatively prime is unbounded, a conclusion that definitely cannot be established by searching. In that respect our generation process (2) and (3) is very powerful.

But it immediately raises the inverse question: can each Pythagorean triple be generated by (2) (with or without all constraints of (3))?

We shall try to answer this question by considering a Pythagorean triple (a, b, c) and then trying to solve (2) viewed as —Diophantine— equations in p, q. Because $x^2 \underline{\text{mod}}\ 4 = 0 \ \vee \ x^2 \underline{\text{mod}}\ 4 = 1$ for all x, in a Pythagorean triple (a, b, c), a and b are not both odd, i.e. without loss of generality we can assume even. b. We observe that p^2 and q^2 are the roots of the equation in x

$$
\begin{array}{ll}
 & (x - p^2)\cdot(x - q^2) = 0 \\
= & \quad \{\text{arithmetic}\} \\
 & x^2 - (p^2 + q^2)\cdot x + p^2\cdot q^2 = 0 \\
= & \quad \{(2)\} \\
 & x^2 - c\cdot x + b^2/4 = 0 \quad ,
\end{array}
$$

the roots of which are $\dfrac{c \pm \sqrt{c^2 - b^2}}{2}$

or, because (a,b,c) is a Pythagorean triple

$$(c \pm a)/2 \quad .$$

Because of even.b, c and a have the same parity, and the above two roots are integer, but since we wish to equate them to p^2 and q^2, the crucial question is: are they squares?

With $p^2 = (c+a)/2$ and $q^2 = (c-a)/2$, we can solve for p and q, i.e. write for integer m, n, u, v

$$p = m \cdot \sqrt{u} \qquad q = n \cdot \sqrt{v}$$

where u and v are "square-free" —i.e. with each prime occurring at most once in its prime factorization— . Because —see (2) and even.b— $p \cdot q$ is integer, $\sqrt{u \cdot v}$ is integer, i.e. $u \cdot v$ is a square; because, moreover, u and v are each square-free, $u = v$, i.e, eliminating v:

$$p = m \cdot \sqrt{u} \qquad q = n \cdot \sqrt{u}$$

and now we have to ensure $u = 1$. The above values for p and q ensure that u is a common factor of $a, b,$ & c. In short:

for any Pythagorean triple (a,b,c)

such that a gcd b gcd c = 1 , there exist integer p, q satisfying (2) .

Remark The condition a gcd b gcd c = 1 can also be formulated less symmetrically, e.g. a gcd b = 1 or b gcd c = 1. It can be generalized by only requiring that that gcd be a square, but I don't think that a generalization to write home about. (End of Remark.)

I had intended to complete this EWD earlier, but I got distracted.

Austin, 10 February 1994

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA