<u>From van IJzeren's correspondence to my aunt & uncle.</u>

Browsing through letters sent to my late aunt dr H.A. van Herk-Kluyver, I found the following theorem and proof in a letter from my late brother-in-law mr dr J. van IJzeren. The theorem is surprising but not interesting; this note is devoted to its proof because it is an elementary and very convincing illustration of the use of the device of the General Solution (which I promoted in EWD1155).

The proof uses two theorems.

(0) A Pythagorean triple that is relatively prime, can be written as p^2-q^2, $2pq$, p^2+q^2. (See EWD1172.)

(1) For prime p, n^p-n is a multiple of p. (Known as "Fermat's Little Theorem", see EWD740.)

The theorem to be proved here —as said: surprising but not interesting— is

(2) For any Pythagorean triple ,i.e. with $a^2+b^2=c^2$, there is a multiple of 7 among (a), (b), $(a-b)$, $(a+b)$

        *   *   *
            *

<u>Proof</u> Because of $a^2+b^2=c^2$, any factor shared by 2 of the numbers is shared by the 3rd, and hence we can restrict ourselves to a,b,c that are relatively prime. We shall do so in what follows.

With $\sqsubseteq$ denoting "divides" and p, q providing (see (0)) the parameters for the General Solution of $a^2 + b^2 = c^2$, we observe

$$7 \sqsubseteq a \;\lor\; 7 \sqsubseteq b \;\lor\; 7 \sqsubseteq a-b \;\lor\; 7 \sqsubseteq a+b$$

$\equiv$ {algebra, prime.7}

$$7 \sqsubseteq ab(a^2 - b^2)$$

$\equiv$ { $a := p^2 - q^2$, $b := 2pq$ }

$$7 \sqsubseteq 2(p^2 - q^2)\, pq\, (p^4 - 2p^2 q^2 + q^4 - 4p^2 q^2)$$

$\equiv$ { $\lnot\, 7 \sqsubseteq 2$, prime.7, algebra }

$$7 \sqsubseteq pq(p^2 - q^2)(p^4 - 6p^2 q^2 + q^4)$$

$\equiv$ { modulo calculus }

$$7 \sqsubseteq pq(p^2 - q^2)(p^4 + p^2 q^2 + q^4)$$

$\equiv$ { algebra }

$$7 \sqsubseteq pq(p^6 - q^6)$$

$\equiv$ { algebra }

$$7 \sqsubseteq p^7 q - pq^7$$

$\equiv$ { Fermat's Little Theorem, modulo calculus, prime.7 }

$$7 \sqsubseteq pq - pq$$

$\equiv$ { $7 \sqsubseteq 0$ }

true.

I don't think I could have proved this theorem without the introduction of p and q.

Austin, 11 January 2002

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