

From van IJzeren's correspondence to my aunt & uncle.

Browsing through letters sent to my late aunt dr H.A. van Herk-Kluyven, 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 EWD1192.)
- (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 $(a), (b), (a-b), (a+b)$
- * *

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

$$\begin{aligned}
 & 7 \varepsilon a \vee 7 \varepsilon b \vee 7 \varepsilon a-b \vee 7 \varepsilon a+b \\
 \equiv & \{ \text{algebra, prime.7} \} \\
 & 7 \varepsilon ab(a^2 - b^2) \\
 \equiv & \{ a := p^2 - q^2, b := 2pq \} \\
 & 7 \varepsilon 2(p^2 - q^2)pq(p^4 - 2p^2q^2 + q^4 - 4p^2q^2) \\
 \equiv & \{ 7 \nmid 2, \text{prime.7, algebra} \} \\
 & 7 \varepsilon pq(p^2 - q^2)(p^4 - 6p^2q^2 + q^4) \\
 \equiv & \{ \text{modulo calculus} \} \\
 & 7 \varepsilon pq(p^2 - q^2)(p^4 + p^2q^2 + q^4) \\
 \equiv & \{ \text{algebra} \} \\
 & 7 \varepsilon pq(p^6 - q^6) \\
 \equiv & \{ \text{algebra} \} \\
 & 7 \varepsilon p^7q - pq^7 \\
 \equiv & \{ \text{Fermat's Little Theorem, modulo calculus, prime.7} \} \\
 & 7 \varepsilon pq - pq \\
 \equiv & \{ 7 \varepsilon 0 \} \\
 & \text{true.}
 \end{aligned}$$

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