# A CONJECTURE RELATING QUARTIC RECIPROCITY AND QUARTIC RESIDUACITY TO PRIMITIVE PYTHAGOREAN TRIPLES

**LARRY TAYLOR**
**85-22 144th Street, Briarwood, New York 11435**

## CONJECTURE

(a) If

$$p = a^2 + b^2 \equiv 1 \pmod 4$$

is prime, $q \equiv 1 \pmod 8$ is prime with $(p/q) = 1$, and $(x,y,z)$ is a primitive Pythagorean triple, then either $a^2 \equiv x^2$ with $b^2 \equiv y^2 \pmod q$ for some $(x,y)$ and $a^2 \equiv -x^2$ with $b^2 \equiv -y^2 \pmod q$ for other $(x,y)$ or $a^2 \not\equiv \pm x^2$ with $b^2 \equiv \pm y^2 \pmod q$ for any $(x,y)$;

$$(\sqrt{p}/q)(\sqrt{q}/p) = 1$$

if and only if the first alternative is true, in which case

$$(z/q)(\sqrt{q}/p) = 1.$$

(b) If $q \equiv 5 \pmod 8$, then either $a^2 \equiv x^2$ with $b^2 \equiv y^2 \pmod{2q}$ for some $(x,y)$ and $a^2 \equiv q - x^2$ with $b^2 \equiv q - y^2 \pmod{2q}$ for other $(x,y)$ or $a^2 \equiv -x^2$ with $b^2 \equiv -y^2 \pmod{2q}$ for some $(x,y)$ and $a^2 \equiv q + x^2$ with $b^2 \equiv q + y^2 \pmod{2q}$ for other $(x,y)$;

$$(\sqrt{p}/q)(\sqrt{q}/p) = 1$$

if and only if the first alternative is true, and

$$(z/q)(\sqrt{q}/p) = 1$$

if and only if $a \equiv x \pmod 2$.

(c) If $q \equiv 3 \pmod 8$, then $a^2 \equiv x^2$ with $b^2 \equiv y^2 \pmod{2q}$ for some $(x,y)$ and $a^2 \equiv q + x^2$ with $b^2 \equiv q + y^2 \pmod{2q}$ for other $(x,y)$;

$$(z/q)(\sqrt{-q}/p) = 1$$

in the first case and

$$(-z/q)(\sqrt{-q}/p) = 1$$

in the second case.

(d) If $q \equiv 7 \pmod 8$, then $a^2 \equiv x^2$ with $b^2 \equiv y^2 \pmod q$ for some $(x,y)$ and

$$(z/q)(\sqrt{-q}/p) = 1.$$

In the following examples, $(x,y,z)$ is the smallest primitive Pythagorean triple that satisfies the congruence:

| $p = a^2 + b^2$ | $(x, y, z)$ | $q$ or $2q$ |
|---|---|---|
| 5 = 1 + 4, | (21, 20, 29) | |
| | (12, 35, 37) | (mod 22); |
| | (77, 36, 85) | |
| | (20, 21, 29) | (mod 38); |
| | (57, 176, 185) | |
| | (12, 5, 13) | (mod 58); |
| | (435, 308, 533) | (mod 31); |
| | (—, —, —) | |
| | (—, —, —) | (mod 41); |
| 29 = 25 + 4, | (5, 12, 13) | |
| | (20, 21, 29) | |
| 41 = 25 + 16, | (5, 12, 13) | |
| | (20, 21, 29) | |
| 101 = 1 + 100, | (21, 20, 29) | |
| | (12, 5, 13) | |
| 109 = 9 + 100, | (21, 20, 29) | |
| | (12, 5, 13) | (mod 10); |
| 13 = 9 + 4, | (3, 4, 5) | |
| | (12, 5, 13) | (mod 6); |
| | (—, —, —) | |
| | (—, —, —) | (mod 17); |
| | (20, 21, 29) | (mod 23); |
| | (7, 24, 25) | |
| | (84, 437, 445) | (mod 58); |
| 17 = 1 + 16, | (21, 20, 29) | |
| | (12, 35, 37) | |
| 29 = 25 + 4, | (77, 36, 85) | |
| | (8, 15, 17) | (mod 26); |
| 17 = 1 + 16, | (39, 80, 89) | |
| | (20, 99, 101) | (mod 38); |
| 53 = 49 + 4, | (112, 15, 113) | |
| | (40, 9, 41) | |
| 149 = 49 + 100, | (7, 24, 25) | |
| | (45, 28, 53) | (mod 17); |
| 41 = 25 + 16, | (615, 728, 953) | |
| | (116, 837, 845) | (mod 122); |
| 61 = 25 + 36, | (87, 416, 425) | |
| | (45, 28, 53) | (mod 41). |

*******