Fermat's Last Theorem

A primitive Pythagorean triple is a set of three positive integers x, y, z where:

$x^2+y^2=z^2$ and x, y, z have no common factor.

for example:

$5, 12, 13$

Theorem

All primitive Pythagorean triples are of the form:

$x=2pq \qquad y=p^2-q^2 \qquad z=p^2+q^2$

where p and q are any positive integers such that:

$p>q$

p and q have no common factor

p and q are not both odd

p and q are not both even

for example $p=7$ and $q=4$ gives $x=56 \quad y=33 \quad z=65$

Proof(?)

We can easily check that:

$(2pq)^2+(p^2-q^2)^2=(p^2+q^2)^2$

But this does not prove that all primitive Pythagorean triples are of this form. Why not?

See Exercise

Fermat's Last Theorem:

There is no set of three positive integers x, y, z where:

$x^3+y^3=z^3$ or $x^4+y^4=z^4$ or $x^5+y^5=z^5$ ...etc

Fermat had the annoying habit of announcing theorems that he had discovered but not providing proofs. It was left to later mathematicians (Euler usually) to supply the proofs. Fermat's last theorem (1637) was the last of these theorems to be proved (1995)

EXERCISE

Prove the following about primitive Pythagorean triples.

1) x and y can't both be even hint: mod 2

2) x and y can't both be odd hint: mod 4

3) z is odd

4) x or y is a multiple of 3 hint: mod 3

5) x or y is a multiple of 4 hint: mod 16

6) x or y or z is a multiple of 5 hint: mod 5

7) xyz is a multiple of 60

SOLUTIONS

1) proof by contradiction

assume x and y are both even

mod 2:

$x=0$ so $x^2=0$

$y=0$ so $y^2=0$

$x^2+y^2=z^2$ so $z^2=0$ so $z=0$ so x,y,z are all even so x,y,z have a common factor

Contradiction

end of mod 2

2) proof by contradiction

assume x and y are both odd

mod 4:

$x=1,3$ so $x^2=1$

$y=1,3$ so $y^2=1$

$x^2+y^2=z^2$ so $z^2=2$ but if $z=0,1,2,3$ then $z^2=0,1$

Contradiction

end of mod 4

3) parts (1) and (2) tell us that x^2+y^2 is odd so z^2 is odd so z is odd

4) proof by contradiction

assume neither x nor y is a multiple of 3

mod 3:

$x=1,2$ so $x^2=1$

$y=1,2$ so $y^2=1$

$x^2+y^2=z^2$ so $z^2=2$ but if $z=0,1,2$ then $z^2=0,1$

Contradiction

end of mod 3

5) proof by contradiction

assume neither x nor y is a multiple of 4

mod 16:

$x = 1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 15$ so $x^2 = 1, 4, 9$

$y = 1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 15$ so $y^2 = 1, 4, 9$

$x^2 + y^2 = z^2$ so $z^2 = 2, 5, 8, 10, 13$

but if $Z = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15$ then $z^2 = 0, 1, 4, 9$

Contradiction

end of mod 16

6) proof by contradiction

assume neither x nor y nor z is a multiple of 5

mod 5:

$x = 1, 2, 3, 4$ so $x^2 = 1, 4$

$y = 1, 2, 3, 4$ so $y^2 = 1, 4$

$x^2 + y^2 = z^2$ so $z^2 = 0, 2, 3$ but if $z = 1, 2, 3, 4$ then $z^2 = 1, 4$

Contradiction

end of mod 5

7) this follows from parts (4), (5) and (6)