

(1)

Let  $p > 2$  be prime and let  $x, y, z$  be relatively prime integers ~~such~~ <sup>such</sup> that  $x^p + y^p + z^p = 0$ .

$$\text{So } (x+y+z) \equiv 0 \pmod{p} \quad (1)$$

This follows from Fermat's Little Theorem.

Square both sides of (1) to obtain

$$(x^2 + y^2 + z^2 + 2xy + 2yz + 2zx) \equiv 0 \pmod{p} \quad (2)$$

Now look at  $(xy + yz + zx)$ . By using (1), we obtain

$$\begin{aligned} (xy + yz + zx) &\equiv (xy - z^2) \pmod{p} \\ &\equiv (yz - x^2) \pmod{p} \\ &\equiv (zx - y^2) \pmod{p} \end{aligned} \quad (3)$$

~~Use  $3 \times (2)$  and  $2 \times (3)$ :~~

~~$$\begin{aligned} 0 &\equiv 3(x^2 + y^2 + z^2) + 6(xy + yz + zx) \pmod{p} \\ &\equiv 3(x^2 + y^2 + z^2) + 2(xy - z^2) \\ &\quad + 2(yz - x^2) \\ &\quad + 2(zx - y^2) \pmod{p} \end{aligned}$$~~

~~Add all three versions of (3):~~

~~$$3(xy + yz + zx) \equiv \left[ (xy - z^2) + (yz - x^2) + (zx - y^2) \right] \pmod{p}$$~~

~~This is~~

~~$$2(xy + yz + zx) + (x^2 + y^2 + z^2) \equiv 0 \pmod{p}$$~~

From (1),  $(x+y)z \equiv -z^2 \pmod{p}$ ,  
Square this:

$$(x^2 + 2xy + y^2)z^2 \equiv z^4 \pmod{p} \quad (4)$$

Similarly,

$$(y^2 + 2yz + z^2)x^2 \equiv x^4 \pmod{p} \quad (5)$$

$$\text{and } (z^2 + 2zx + x^2)y^2 \equiv y^4 \pmod{p} \quad (6)$$

Subtract (4) from (2):

$$z^2 + 2zx + 2yz \equiv -z^2 \pmod{p}$$

$$2z^2 + 2zx + 2zy \equiv 0 \pmod{p}$$

This is  $2z \times (1)$ .

$$\text{Let } S \equiv (xy + yz + zx) \pmod{p} \quad (7)$$

$$\text{This } S \equiv (xy - z^2) \pmod{p} \quad (8)$$

$$\equiv (yz - x^2) \pmod{p} \quad (9)$$

$$\equiv (zx - y^2) \pmod{p} \quad (10)$$

These use  $(x+y)z \equiv -z^2 \pmod{p}$ , etc,  
from (1).

$$\text{Add (8) + (9) + (10) =}$$

$$3S \equiv (xy + yz + zx - x^2 - y^2 - z^2) \pmod{p}$$

(3) -

look at (1) and  $(x+y-z) \equiv -2z \pmod{p}$  — (11)

Square both sides of (11):

$$(x^2 + y^2 + z^2 + 2xy - 2yz - 2zx) \equiv +4z^2 \pmod{p}$$

Using  $y+x \equiv -z \pmod{p}$  from (1) — (12)

$$(x^2 + y^2 + z^2 + 2xy + 2z^2) \equiv 4z^2 \pmod{p} \text{ (12) becomes}$$

This is

$$(x^2 + y^2 + z^2 + 2xy) \equiv 2z^2 \pmod{p} \text{ — (13)}$$

Similarly,

$$(x^2 + y^2 + z^2 + 2yz) \equiv 2x^2 \pmod{p} \text{ — (14)}$$

$$\text{and } (x^2 + y^2 + z^2 + 2zx) \equiv 2y^2 \pmod{p} \text{ — (15)}$$

~~(13) is~~

$$\text{By (8), } xy \equiv (S+z^2) \pmod{p} \text{ — (8)}$$

So in (12), we get  $(x^2 + y^2 + z^2 + 2S) \equiv 0 \pmod{p}$ .

$$(13) \text{ is } (x^2 + y^2 - z^2 + 2xy) \equiv 0 \pmod{p} \text{ — (13')}$$

This by (8) is

$$(x^2 + y^2 + S + xy) \equiv 0 \pmod{p} \text{ — (16)}$$

However, (13) also gives from (13') and (8):

$$(x^2 + y^2 + 2S + z^2) \equiv 0 \pmod{p} \text{ KNOWN!}$$

An analogue of (16) is

$$(y^2 + z^2 + S + yz) \equiv 0 \pmod{p} \text{ — (17)}$$

Subtract

$$(16) - (17) : (x^2 - z^2 + xy - yz) \equiv 0 \pmod{p} \quad (4)$$

$$\text{This is } (x-z)(x+z+y) \equiv 0 \pmod{p} \text{ KNOWN!} \quad (18)$$

Now look at

$$(x^2 + y^2 + z^2 + 2xy + 2yz + 2zx) \equiv 0 \pmod{p} \quad (2)$$

and multiply by 3:

$$3(x^2 + y^2 + z^2) + (6xy + 6yz + 6zx) \equiv 0 \pmod{p}$$

Add (8) + (9) + (10):

$$3S \equiv (xy + yz + zx - x^2 - y^2 - z^2) \pmod{p}$$

$$\equiv (S - x^2 - y^2 - z^2) \pmod{p}$$

$$2S \equiv (-x^2 - y^2 - z^2) \pmod{p}$$

$$6S \equiv 3(-x^2 - y^2 - z^2) \pmod{p}$$

Put it in (2) to obtain  $0 \equiv 0 \pmod{p}$  KNOWN!