D7

gcd!
$\downarrow$
WLOG $(x,y,z)=1$

$3x^2+5y^2=7z^2$

reduce mod 7 $\qquad 3x^2 \underset{7}{\equiv} -5y^2 \underset{7}{\equiv} 2y^2$

$5\cdot 3x^2 \equiv x^2 \underset{7}{\equiv} 5\cdot 2y^2 \equiv 3y^2$

$y \underset{7}{\equiv} 0 \Rightarrow x \underset{7}{\equiv} 0 \Rightarrow 7^2 \mid 3x^2+5y^2 = 7z^2 \Rightarrow 7 \mid z^2 \Rightarrow 7 \mid z$

So $y \underset{7}{\not\equiv} 0$ so $y^6 \underset{7}{\equiv} 1$ so $y(\underbrace{y^5}_{=\alpha}) \underset{7}{\equiv} 1$

so $x^2\alpha^2 = (x\alpha)^2 = c^2 \underset{7}{\equiv} 3y^2\alpha^2 = 3(y\alpha)^2 \underset{7}{\equiv} 3(1)^2 \underset{7}{\equiv} 3$

so $c^2 \underset{7}{\equiv} 3$ for some c.

But! $1^2\equiv 1$ $\quad 2^2\equiv 4$ $\quad 3^2 \equiv 2$ ~~...~~ $\Rightarrow$ can't hit $\underline{3}$.
$4^2\equiv 2$ $\quad 5^2\equiv 4$ $\quad 6^2\equiv 1$

$x^4+y^4=z^2$ if $g \mid x,y,z$ then $\left(\frac{x}{g}\right)^4+\left(\frac{y}{g}\right)^4=\left(\frac{z}{g^2}\right)^2$

$\Longrightarrow$ wolog $(x,y,z)=1$

$\Longrightarrow (x,y)=1$

$x^2=2rs \quad \underset{\text{odd}}{y^2}=r^2-s^2 \quad z=r^2+s^2$

NOTE $\Longrightarrow (r,s)=1$

note $s^2+\underset{\text{odd}}{y^2}=r^2 \Longrightarrow s$ even, r odd

$x^2=r(2s) \qquad (r,2s)=1$

$\Longrightarrow r=u^2,\ 2s=v^2 \Longrightarrow v$ even

$\Longrightarrow s=2w^2$

$y^2=r^2-s^2 \Longrightarrow y^2+s^2=r^2=u^4$

$\Longrightarrow y^2+4w^4=r^2=u^4$ NOTE (Check! $(y,w)=1$)

$\Longrightarrow y^2+4w^4=u^4$ has a solution

$\underset{\text{odd}}{y^2}+(2w^2)^2=(u^2)^2$

$\Longrightarrow y=a^2-b^2 \qquad 2w^2=2ab \qquad u^2=a^2+b^2$

$\Longrightarrow w^2=ab$ NOTE Check! $(a,b)=1$

$\Longrightarrow a=\alpha^2,\ b=\beta^2$

$\Longrightarrow u^2=\alpha^4+\beta^4$ (wlog β even)

But! $x^2=2rs>s=2w^2=2ab\geq b=\beta^2$

$\Longrightarrow \beta<x$, i.e., this is a "smaller" solution!

$$x^4+y^4=z^4 \implies x^4+y^4=(z^2)^2=w^2$$

If $\exists$ solution with $x,y>0$ then

WMA $(x,y)=1$ (If $d|x, d|y$, then $d^4|x^4+y^4=w^2 \Rightarrow d^2|w$, and

$$\left(\frac{x}{d}\right)^4+\left(\frac{y}{d}\right)^4=\left(\frac{w}{d^2}\right)^2 .)$$

$$\boxed{x^4+y^4=w^2}$$

Then $(x^2)^2+(y^2)^2=w^2$ $(x^2,y^2)=1$ WMA x^2 odd, y^2 even

Then $x^2=r^2-s^2$, $y^2=2rs$, $w=r^2+s^2$ for some $r,s>0$

Note: $x^2+s^2=r^2$; $(r,s)=1$ (o/w $d|r, d|s \Rightarrow d^2|x, d^2|y \Rightarrow (x,y)\neq 1$)

$\implies (x,s)=1$ (o/w $d|x, d|s \Rightarrow d^2|x^2+s^2=r^2 \Rightarrow d|r$)

x^2 odd $\Rightarrow$ x odd $\Rightarrow$ s even, r odd

$(r,s)=1 \implies (r,2s)=1$ $y^2=r(2s) \Rightarrow r=u^2,\ 2s=v^2=(2t)^2$

$\Rightarrow s=2t^2$

$x^2+s^2=r^2$ x odd, s even $\implies$

$x=a^2-b^2$, $s=2ab$, $r=a^2+b^2$ for some $a,b>0$

Note: $(a,b)=1$ (o/w $d|a, d|b \Rightarrow d^2|2ab=s, d^2|a^2+b^2=r \Rightarrow (r,s)\neq 1$)

$2t^2=s=2ab \Rightarrow t^2=ab \Rightarrow a=\alpha^2, b=\beta^2$ some $\alpha,\beta>0$

$\implies \alpha^4+\beta^4=a^2+b^2=r=u^2$, so $\boxed{\alpha^4+\beta^4=u^2}$ Note: $(\alpha,\beta)=1$

But: $0<\alpha<\alpha^2=a<2ab=s<2rs=y^2$ so $\alpha^2<y^2 \Rightarrow \alpha<y$

$0<\beta<\beta^2=b<2ab=s<2rs=y^2$ $\beta^2<y$ $\beta<y$

So whichever one is even is smaller than y.

So a solution to $x^4+y^4=w^4$ with y even and smallest can't exist $\Rightarrow$ no solution with $y>0$ can exist.

Another proof by infinite descent

* $\boxed{x^2+y^4=z^4}$, i.e. $x^2+(y^2)^2=(z^2)^2$, has no solutions with $x,y,z>0$.

Pf: Suppose we have a solution. If $p|x$, $p|y$, then $p|x^2+y^4=z^4$, so $p|z$. Then $p^4|z^4-y^4=x^2$, so $p^2|x$, so $\left(\frac{x}{p^2}\right)^2+\left(\frac{y}{p}\right)^4=\left(\frac{z}{p}\right)^4$ is a solution. So WMA $(x,y)=(x,y^2)=1$.

Then (x,y^2,z^2) is a primitive Pythagorean triple. Unlike our other example, we will need to treat the cases x even/y^2 odd and x odd/y^2 even differently; we cannot simply interchange x and y.

We treat x odd, y^2 even first. There are $r,s>0$ so that
$x=r^2-s^2$, $y^2=2rs$, $z^2=r^2+s^2$, with $r-s$ odd. $(x,y)=1$ implies $(r,s)=1$.
WLOG r is even, s is odd (the opposite case is similar) (just put the 2 in the other place.)
Then $(2r,s)=1$ so $y^2=(2r)s \implies 2r=u^2$, $s=v^2$ for some $u,v>0$.
Then u is even, so $2r=(2w)^2=4w^2$ so $r=2w^2$. $(r,s)=1$ implies $(w,v)=1$.
$z^2=r^2+s^2$ implies that there are $\alpha,\beta>0$ so that
$r=2\alpha\beta=2w^2$, $s=\alpha^2-\beta^2$. $(r,s)=1 \implies (\alpha,\beta)=1$. Then
$\alpha\beta=w^2 \implies \alpha=a^2$, $\beta=b^2$ for some $a,b>0$. Then
$s+\beta^2=\boxed{u^2+b^4=a^4}=\alpha^2$. But $a<a^2=\alpha<2\alpha\beta=r<\sqrt{r^2+s^2}=z$, so
$a<z$. Note that $(\alpha,\beta)=1$ implies $(a,b)=1$, which implies $(u,b)=1$.
But note: u is even, so b is odd. We have ~~state~~ found a smaller
solution to the other case! Remember this; we will look at the
other case now.

If $x^2+(y^2)^2=(z^2)^2$, $(x,y^2)=(x,y)=1$, x even, y odd, then
there are $r,s>0$ so that $x=2rs$, $y^2=r^2-s^2$, $z^2=r^2+s^2$, with
$r-s$ odd. $(x,y)=1$ implies $(r,s)=1$, so $(y,s)=1$.
$y^2+s^2=r^2$ and y odd implies s is even, r is odd.

Then $y^2+s^2=r^2$, $r^2+s^2=z^2$, so $y^2+2s^2=z^2$, so $\left(\frac{y}{z}\right)^2+2\left(\frac{s}{z}\right)^2=1$

One solution to $A^2+2B^2=1$ is $A=1, B=0$; to find all other rational solutions, set $B=r(A-1)$, $r\in\mathbb{Q}$ ($A=1$ is our first solution)

Then $A^2+2(r(A-1))^2=1$, so $(A-1)((A+1)+2r^2(A-1))=0$. So $A=1$ or $A+1+2r^2A-2r^2=0$, i.e. $A=\frac{2r^2-1}{2r^2+1}$. Then $B=r\left(\frac{2r^2-1}{2r^2+1}-1\right)=\frac{-2r}{2r^2+1}$. Setting $r=\frac{-a}{b}$ ($a>b>0$ gives positive solutions) gives $A=\frac{2a^2-b^2}{2a^2+b^2}$, $B=\frac{2ab}{2a^2+b^2}$, so

$y=2a^2-b^2$, $s=2ab$, and $z=2a^2+b^2$ for some $a,b>0$

Plugging into $y^2+s^2=r^2$ gives $r^2=(2a^2-b^2)^2+(2ab)^2$
$$=4a^4-4a^2b^2+b^4+4a^2b^2=(2a^2)^2+(b^2)^2$$
r odd implies b^2 odd, which implies b is odd

WMA $(a,b)=1$, otherwise we can divide numerator and denominator of A and B by $(a,b)^2$ to replace a,b by $a/(a,b)$, $b/(a,b)$.

Then $(b^2,2a^2)=1$, so $(2a^2,b^2,r)$ is a primitive Pythagorean triple, so there are $u,v>0$ so that $2a^2=2uv$, $b^2=u^2-v^2$, $r=u^2+v^2$.

$(a,b)=1$ implies $(u,v)=1$, and $a^2=uv$ implies that $u=\alpha^2$, $v=\beta^2$ for some $\alpha,\beta>0$. Then $b^2=\alpha^4-\beta^4$, i.e. $\boxed{b^2+\beta^4=\alpha^4}$. $(\alpha,\beta)=1$, so $(b,\beta)=1$.

But $\alpha<\alpha^2=u<2uv=2a^2<2a^2+b^2=z$, so $\alpha<z$. Again, however, b is odd, so β is even, and we have found a smaller solution to the other case! But taken together, if we have a solution to (*) with $x,y,z>0$ and z smallest, then no matter which case it is, we can find a new solution with smaller z, a contradiction. So there are no solutions to $x^2+y^4=z^4$ with $x,y,z>0$.

p an odd prime, then $\exists\, x,y$ s.t.

$$(*)\quad \boxed{x^2+y^2 \underset{p}{\equiv} -1}$$

Look at $\{ \cancel{m} \; 0 \le n \le p-1 : x^2 \underset{p}{\equiv} n$ has a solution $\} = H$

note that since $(2,p-1)=2$, every eqn $x^2 \underset{p}{\equiv} n$ that <u>has</u> a solution has ($n=0$ 1 one solution ~~or~~) <u>two</u> solutions.

$n \in H \implies p-n-1 \notin H$.

<u>If</u> $(*)$ has no solutions then

$\longrightarrow$ $x^2 \underset{p}{\equiv} -1$ has <u>no</u> solution $\implies \boxed{p \underset{4}{\equiv} 3}$

$\hookrightarrow (-1)^{\frac{p-1}{2}} \underset{p}{\equiv} (-1) \implies \frac{p-1}{2}$ is <u>odd</u>

$p-1 = 2(2k+1)$

$p = 4k+3$ ✓

Ie. $\cancel{n}$

$x^2 \underset{p}{\equiv} n$ has soln $\implies n^{\frac{p-1}{2}} \underset{p}{\equiv} 1 \implies (p-n-1)^{\frac{p-1}{2}} \underset{p}{\equiv} -1$

$$-1 \equiv (p-(n+1))^{\frac{p-1}{2}} \underset{p}{\equiv} (-1)^{\frac{p-1}{2}}(n+1)^{\frac{p-1}{2}}$$

$$\equiv (-1)(n+1)^{\frac{p-1}{2}}$$

$\implies (n+1)^{\frac{p-1}{2}} \equiv 1 \implies x^2 \underset{p}{\equiv} n+1$ has soln!

Local vs global solutions

If $f(x_1, \dots, x_n) = 0$ has solutions with $x_i \in \mathbb{Z}$

then it certainly has solutions with $x, y, z \in \underline{\mathbb{R}}$. Also,

$f(x_1, \dots, x_n) \underset{N}{\equiv} 0$ has a solution for any N

(use the solutions x, y, z from $\underline{\mathbb{Z}}$!)

Any solution to the latter kind of equation is called a <u>local</u> solution to $f = 0$. By analogy, a solution to $f = 0$ with $x_i \in \mathbb{Z}$ is called a <u>global soln</u>.

So global soln $\Longrightarrow$ local soln for $\mathbb{R}$, and for any N.

So no local soln (for any <u>one</u> instance)
$\Longrightarrow$ <u>no</u> global solution.

This can be very effective in showing that a Diophantine eqn has <u>no</u> solutions!

But it isn't perfect: $x^4 - 17 = 2y^2$ always has a <u>local</u> solution, but has no <u>global</u> ones

$3(3^{k-1}-1)$

$x^2+y^2+z^2=-1$

$\boxed{x^2+y^2+z^2+w^2=-1}$ no $\mathbb{R}$, all $\mathbb{Z}_n$.

$2x^2+3y^2=-1$

$2x^2+3y^2\equiv_n -1$

$\boxed{2^t\equiv_n 3}$?

$5^k\equiv_n 3$

$3^{\phi(n)}\equiv 1$

$3^{\phi(n)+1}\equiv 3$

$\boxed{3^n\equiv 3}$

$x^2+2y^2=p$

3 3

$\boxed{x^2+y^2\equiv_n 3}$ NO not ~~solvable for~~ $\ast\, 4|n$
~~solvable for all other n (?), and for $\mathbb{R}$~~.

$N\equiv_n 3$

$N\equiv_4 1$ ✓

$x^2+y^2=kn+3=N$

p odd prime, then $x^2+y^2 \underset{p}{\equiv} -1$ has a solution

If $x^2 \underset{p}{\equiv} n$ then $(p-x)^2 \underset{p}{\equiv} n$

~~$x^2 - n \underset{p}{\equiv} 0$~~

OTOH, $x^2 \underset{p}{\equiv} y^2 \Rightarrow (x-y)(x+y) \underset{p}{\equiv} 0 \Rightarrow p \mid x-y$ $(y=x)$
or $p \mid x+y$ $(y=p-x)$

$0 \le x, y \le p-1$.

$\Longrightarrow$ for exactly half of $1 \le n \le p-1$ there are solutions to $x^2 \underset{p}{\equiv} n$

If $x^2+y^2 \underset{p}{\equiv} -1$ has no solution, then <u>Note</u> $x^2 \underset{p}{\equiv} -1$ has no solution

$x^2 \underset{p}{\equiv} n$ has solution $\Longleftrightarrow$ $x^2 \equiv (p-n)-1$ has no solution.

for all $1 \le n \le p-1$, <u>But</u>! $x^2 \underset{p}{\equiv} n$ has a solution $\Longleftrightarrow$

$n^{\frac{p-1}{2}} \underset{p}{\equiv} 1$. [Note: p prime $\Rightarrow n^{p-1} \underset{p}{\equiv} 1 \Rightarrow n^{\frac{p-1}{2}} \equiv \pm 1$.]

So $n^{\frac{p-1}{2}} \underset{p}{\equiv} 1 \Longleftrightarrow (p-(n+1))^{\frac{p-1}{2}} \underset{p}{\equiv} -1$.

<u>But</u>! $p-(n+1) \equiv -(n+1)$ so $-1 \equiv (p-(n+1))^{\frac{p-1}{2}} \underset{p}{\equiv} (-(n+1))^{\frac{p-1}{2}}$

$\underset{p}{\equiv} (-1)^{\frac{p-1}{2}} (n+1)^{\frac{p-1}{2}}$

$\underset{p}{\equiv} (-1)(n+1)^{\frac{p-1}{2}} \equiv$ ~~-1~~

$\Longrightarrow (n+1)^{\frac{p-1}{2}} \underset{p}{\equiv} 1$

$\Longrightarrow x^2 \underset{p}{\equiv} n+1$ <u>has</u> a solution

Since $x^2 \underset{p}{\equiv} 1$ has a solution, thus $\Rightarrow$ $x^2 \equiv 2$ does $\Rightarrow$ $x^2 \equiv 3$ done

$\Longrightarrow$ they <u>all</u> do, <u>contrad</u>.