Every $n \in \mathbb{N}$ is the sum of four squares

$$(x^2+y^2+z^2+w^2) + (x_1^2+y_1^2+z_1^2+w_1^2)$$
$$= (xx_1+yy_1+zz_1+ww_1)^2 + (xy_1-yx_1+wz_1-zw_1)^2$$
$$+ (xz_1-zx_1+yw_1-wy_1)^2 + (xw_1-wx_1+zy_1-yz_1)^2$$

p an odd prime

If $0 \le x, y \le \frac{p-1}{2}$, $x \ne y$

$\Longrightarrow \quad x^2 \not\equiv_p y^2$

$x^2 \equiv_p y^2 \Longrightarrow p \mid x^2-y^2 = (x-y)(x+y) \Longrightarrow p \mid x-y$ or $p \mid x+y$

$\Longrightarrow x \equiv_p y$ or $x \equiv_p -y$

$\Longrightarrow x = y$ or $x = p-y$

$\Longrightarrow x = y$ or $x+y = p$ $\quad ※$.

For any a, $\exists\ 0 \le x, y \le \frac{p-1}{2}$ with $x^2+y^2 \equiv_p a$

Pf: ~~the~~ if not then $x^2 \not\equiv_p a-y^2$ for any x, y

But for $0 \le x \le \frac{p-1}{2}$, then $x^2 \pmod p$ are distinct

& the $a-y^2$ are distinct $(\text{mod } p)$

But there are $2\left(\frac{p+1}{2}\right) = p+1$ of them, so two are the same $\Longrightarrow$ one of x^2 and one of $a-y^2$ are $\equiv_p$. ∎

Every $n \in \mathbb{N}$ can be expressed as

$$n = x^2+y^2+z^2+w^2 \quad \text{for} \quad x,y,z,w \in \mathbb{Z}.$$

Pf. Suffices to check for primes p.

$p=2 \qquad 2 = 1^2+1^2+0^2+0^2$

Look at odd primes

By above, $\exists$ $0 \le x,y \le \frac{p-1}{2}$ with

$p \mid x^2+y^2+1$ but $x^2+y^2+1 \le \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1$

$= \frac{1}{2}(p-1)^2+1 < p^2$

So $x^2+y^2+1 = mp$ for some $m<p$.

$x^2+y^2+1^2+0^2$ we proceed to eliminate m!

$x^2+y^2+z^2+w^2 = mp$ with $m<p$

m even $\Rightarrow$ an even # of x,y,z,w are even

WLOG none, x,y, or all then

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 = \frac{m}{2}p$$

now suppose m is odd then choose $0 \le x_1, y_1, z_1, w_1 < m$ with $|x_1|, \ldots |w_1| \le \frac{m}{2}$

with $m \mid x-x_1, y-y_1, z-z_1, w-w_1$ then

$x_1^2+y_1^2+z_1^2+w_1^2 \equiv_m x^2+y^2+z^2+w^2 \equiv_m 0$ so

$x_1^2 + \ldots + w_1^2 = mm'$ with $|x_1^2 \ldots| \le |x_1^2 \ldots| \le 4\left(\frac{m^2}{4}\right)$

$\le m^2 = m^2$

$(mp)(m'p)$
$\quad\,\,''$

Then $(x^2 + \cdots + w^2)(x_1^2 + \cdots w_1^2)$

$= a^2 + b^2 + c^2 + d^2$

but $\quad a = xx_1 + yy_1 + zz_1 + ww_1 \equiv_m x^2 + \cdots + w^2 \equiv_m 0$

$\quad\;\; b = xy_1 - yx_1 + wz_1 - zw_1 \equiv_m xy - yx + wz - zw \equiv_m 0$

etc.

so $m \mid a, b, c, d$ so

$m'p = \left(\frac{a}{m}\right)^2 + \cdots + \left(\frac{d}{m}\right)^2 \quad$ with $\quad m' < m$!

Done by induction.

$$
\begin{aligned}
&(x_1^2+y_1^2+z_1^2+w_1^2)(x_2^2+y_2^2+z_2^2+w_2^2) \\
&= (x_1x_2 + y_1y_2 + z_1z_2 + w_1w_2)^2 \\
&\quad + (x_1y_2 - x_2y_1 + z_2w_1 - z_1w_2)^2 \\
&\quad + (x_1z_2 - x_2z_1 + y_1w_2 - y_2w_1)^2 \\
&\quad + (x_1w_2 - x_2w_1 + y_2z_1 - y_1z_2)^2
\end{aligned}
$$