Theorem.

every positive integer is the sum of four squares.

Proof.

Lemma $(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = z_1^2+z_2^2+z_3^2+z_4^2$

where
$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$
$$z_2 = x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3$$
$$z_3 = x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2$$
$$z_4 = x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2$$
(通过坐标系变换易证)

则只需证 Theorem 对所有素数成立，$p=2$ 显然

下设 p 为素数

考虑 $\{a^2 \mid a \in \{0, 1, \cdots \frac{p-1}{2}\}\}$ 有 $\frac{p+1}{2}$ 同余类

$\{-1-b^2 \mid b \in \{0, 1, \cdots, \frac{p-1}{2}\}\}$ 有 $\frac{p+1}{2}$ 同余类

则必存在 $a^2+b^2+1 \equiv 0 \pmod p$

则 $\exists n$, $np = a^2+b^2+1$, $n \in [1, p)$

$\exists m$ s.t. 最小的 $m \in [1, n]$, $mp = x_1^2+x_2^2+x_3^2+x_4^2$

Claim. $m=1$

proof of the claim.

by contradiction, $1 < m \le n$

设 $y_i \equiv x_i \pmod m$ for $i \in \{1,2,3,4\}$ $y_i \in (-\frac{m}{2}, \frac{m}{2}]$

则 $\sum y_i^2 \equiv \sum x_i^2 \equiv mp \equiv 0 \pmod m$

令 $mr = \sum y_i^2$，则 $mr \le 4\cdot(\frac{m}{2})^2 = m^2$

if $r = m$, $y_i = \frac{m}{2}$ $mp = m^2 \mod m^2$，与 p 素性相矛盾

因此 $r < m$

则 $(mp)\cdot(mr) = \sum x_i^2 \sum y_i^2 = \sum z_i^2$

易得 $z_i \equiv 0 \pmod m$ $z_i = w_i m$

则 $r\cdot p = \sum w_i^2$，与 m 的最小性矛盾.

Q.E.D.

Q.E.D.