

First suppose m is a square in R . Then

$$(*) \quad mI = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix}$$

for some $a, b, c, d \in \mathbb{Z}$ with $n \mid b$. Therefore, $m = a^2 + bc \equiv a^2 \pmod{n}$. Conversely, if $m \equiv a^2 \pmod{n}$ for some $a \in \mathbb{Z}$, then $m = a^2 + nc$ for some c , and $(*)$ holds with $b = n$ and $d = -a$.