

Question

Let $n \geq 4$ be an integer that is not prime. Show that the integers modulo n , \mathbf{Z}_n , is not a field.

Answer

Write n as a product $n = a \cdot b$, where $2 \leq a, b < n$, so that a and b are not equal in \mathbf{Z}_n . Then, in \mathbf{Z}_n , the product $a \cdot b$ is 0, being a multiple of n . However, if \mathbf{Z}_n were a field, then a would have a multiplicative inverse a^{-1} , and we could multiply both sides of $a \cdot b = 0$ on the left to obtain $a^{-1} \cdot a \cdot b = a^{-1} \cdot 0$, which simplifies to $b = 0$. This contradicts the choice of b to satisfy $2 \leq b < n$, and so a has no multiplicative inverse, contradicting the definition of a field.