If \( p \) is any odd prime number and \( c \) is any odd number less than \( p \), then there must exist a positive number \( c' \) less than \( p \), such that \( cc' = -2 \mod p \)

Prashanth R. Rao

Proof:

Let \( p \) be an odd prime. Let \( c \) be any odd number less than \( p \). Therefore there must exist an even number \( 2b \) such that \( c + 2b = p \). Please note than \( 2b \) is less than \( p \) and therefore \( b \) is less than \( p \).

Special case if \( 2b = 2 \)

If \( 2b = 2 \), then \( c + 2 = p \) or \( c(1) + 2 = p \) and therefore \( c(1) = -2 \mod p \) and therefore \( c' = 1 \).

All other values of \( 2b \), where \( 2 < 2b < p \):

\[ c + 2b = p \quad \text{..........................(I)} \]

Let \( c' \) be a number less than \( p \) such that \( bc' = 1 \mod p \)

(Since \( p \) is prime, there must exist unique pair of numbers \( b \) and \( c' \) both greater than 1 and both less than \( p \), such that their product \( bc' = 1 \mod p \)).

Multiplying (I) by \( c' \) gives

\[ cc' + 2bc' = pc' \]

Therefore

\[ cc' + 2(1) = 0 \mod p \]

or

\[ cc' = -2 \mod p \]