26. Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

Proof:

Consider $k = n-1 \in U(n)$, recall that k represents the equivilence class of integers modulo n. Note that if $n > 2$

$$n-1 \pmod n = -1 \pmod n.$$

Hence:

$$(n-1 \bmod n)^2 = (-1 \bmod n)(-1 \bmod n) = (-1)^2 \bmod n$$
$$= 1 \bmod n$$

$\therefore$ If $n > 2$ $k = n-1 \neq 1$ is such that $k^2 = 1$.

Version 2:

$$(n-1)^2 \bmod n = n^2 - 2n + 1 \bmod n$$
$$= 1 \bmod n \quad \text{since } n = 0 \bmod n$$

Either version is fine.

32. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$.

Proof: G has even order, $\therefore |G| \geq 2$.

Since G is a group $e \in G$. Let $n = |G|$, suppose $b \in G$ is s.t. $b^2 \neq e$ and $b \neq e \Rightarrow b^{-1} \neq b$

$\therefore$ the set $S = \{ b \in G \mid b^2 \neq e, b \neq e \}$ has an even number of elements as for any $b \in S$ we must also have an element $b^{-1} \in G$, with $b^{-1} \neq b$, $\therefore b^{-1} \in S$.

Since n is even then $n-1$ is odd so the number of elements in S is strictly less than $n-1$, i.e. $|S| < n-1$, (since $e \notin S$ and $|S|$ is even).

$\therefore$ There exists at least one $c \in G$, $c \neq e$ such that $c = c^{-1}$
$\Rightarrow c^2 = e$.

Note: many variations of this are possible, the main point is that there are an odd number of elements which are not the identity, and there must be an even number of non-identity elements which are not their own inverses, so this means there must be at least one element which is its own inverse.

49. Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

Proof:

we know $a^4 b = ba$, re writing this we have

$a^3 \cdot ab = ba$, but $a^3 = e$

$\therefore$ we have $ab = ba$. ∎