GROUPS

DEFINITION:

A group is a set G which is equipped with an operation $*$ and a special element $e \in G$, called the identity, such that

(i) the associative law holds: for every $x, y, z \in G$,

$$x * (y * z) = (x * y) * z;$$

(ii) $e * x = x = x * e$ for all $x \in G$;

(iii) for every $x \in G$, there is $x' \in G$ with

$$x * x' = e = x' * x.$$

THEOREM

If p is a prime and $p \equiv 1 \bmod 4$, then there is an integer m with

$$m^2 \equiv -1 \bmod p.$$

PROOF

If $G = (Z_p)^\times$ is the multiplicative group of nonzero elements in Z_p, then $|G| = p - 1 \equiv 0 \bmod 4$; that is, 4 is a divisor of $|G|$. By Proposition 2.59, G contains a subgroup S of order 4. By Exercise 2.52, either S is cyclic or $a^2 = 1$ for all $a \in S$. Since Z_p is a field, however, it cannot contain 4 roots of the quadratic $x^2 - 1$. Therefore, S is cyclic, say, $S =< [m] >$, where $[m]$ is the congruence class of $m \bmod 4$. Since $[m]$ has order 4, we have $[m^4] = [1]$. Moreover, $[m^2] \neq [1]$ (lest $[m]$ have order $\leq 2 < 4$), and so $[m^2] = [-1]$, for $[-1]$ is the unique element in S of order 2. Therefore, $m^2 \equiv -1 \bmod p$. ■