A Qualifying Exam Question

Show that every element in a finite field F is a sum of two squares in that field.[1]

We approach the question in cases:

F is characteristic 2: In characteristic 2, $a^2 + b^2 = (a + b)^2$, so the map $\phi : F \to F$ defined as $\phi(x) = x^2$ is a ring homomorphism. The only ideals of a field (and thus the only possible kernels for this ring homomorphism) are the zero ring or the whole ring. We see that $\phi(1_F) = 1_F \neq 0_F$, so the kernel is not the whole field. We thus see that the kernel is trivial, so this map is injective between to finite sets, whence this map is surjective. We thus see that every element in a field of characteristic 2 is a square, so every element is trivially a sum of squares (e.g., by adding the square 0_F).

Now, a useful general proposition:

Proposition. *If G is a finite group, and $A, B \subset G$ such that $|A| + |B| > |G|$, then $AB = \{ab \mid a \in A, b \in B\} = G$.*

Proof. Let $g \in G$. We want to show there is an $a \in A$ and $b \in B$ so that $g = ab$, or otherwise stated $gb^{-1} = a$. Examine $gB^{-1} = \left\{gb^{-1} \in B\right\}$. Multiplication by the group element g and taking the inverse are one-to-one maps, so $\left|gB^{-1}\right| = |B|$. Thus, we know that $|A| + \left|gB^{-1}\right| > |G|$, so $A \cap gB^{-1} \neq \emptyset$. Take a and gb^{-1} in this intersection; we then have $a = gb^{-1}$, so $ab = g$ as desired. □

F is not characteristic 2: Again examine the square map ϕ we see that for $a, b \in F$ we have $\phi(a) = \phi(b)$ if and only if $a^2 - b^2 = (a - b)(a + b) = 0$, thus $a = b$ or $a = -b$. We thus see that the map ϕ restricted to $F^\times$ is sends two distinct elements to a single square. This tells us that exactly one half of the elements in $F^\times$ are squares. The element 0_F is also a square, so there are $(q-1)/2+1 = (q+1)/2$ elements in F that are squares; let's call this set S. Consider the group F under the addition operation, and note that $|S| + |S| > |F|$, so $S + S = F$ by the above proposition. We thus have that every element in F is a sum of two squares.

[1] This proof is due to Henry Mann (1905-2000).