Rutgers University: Algebra Written Qualifying Exam
August 2015: Problem 1 Solution

Exercise. Let $\mathbb{F}$ be a finite field of order q, with q odd. Show that the following are equivalent:

(a) the equation $x^2 = -1$ has a solution in $\mathbb{F}$

(b) $q \equiv 1 \mod 4$
Hint: work with the multiplicative group $\mathbb{F}^\times$ of nonzero elements in $\mathbb{F}$

Solution.

Since $\mathbb{F}$ is a finite field of order q, $F \cong \mathbb{Z}_q$, q prime
Fermat's Little Theorem: $a^{q-1} \equiv 1 \mod q$, $\forall a \in \mathbb{Z}_q^*$
Since q is odd, $q \equiv 1$ or $3 \mod 4$.

Case 1: $q \equiv 1 \mod 4 \implies q = 4k+1$ for some $k \in \mathbb{N}$
$a^{4k} = a^{q-1} \equiv 1 \mod q$ by Fermat's Little Theorem
$\implies (a^{2k})^2 \equiv 1 \mod q$
$\implies a^{2k} \equiv \pm 1 \mod q$
But a is generator of $\mathbb{Z}_q^*$
$\implies o(a) = q - 1 = 4k$
$\implies a^{2k} \not\equiv 1 \mod q$
$\implies a^{2k} \equiv -1 \mod q$
$\implies x^2 \equiv -1$ has a solution in $\mathbb{F}$

Case 2: $q \equiv 3 \mod 4 \implies q = 4k+3$ for some $k \in \mathbb{Z}_{\geq 0}$
$a^{4k+2} = a^{q-1} \equiv 1 \mod q$ by Fermat's Little Theorem
$\implies (a^{2k+1})^2 \equiv 1 \mod q$
$\implies a^{2k+1} \equiv -1 \mod q$
a is generator of $\mathbb{Z}_q^*$ and $2k+1$ is odd.
$\implies x^2 \equiv -1$ has no solutions in $\mathbb{F}$

Thus, $x^2 \equiv -1$ has a solution in $\mathbb{F} \iff q \equiv 1 \mod 4$