Show that any element in a finite field F can be written as the sum of two squares.

Let F be a finite field of size q. We will use the following facts, which are easy generalisations of Questions 9 and 10 in Assignment 1:

- If $Char(F) = 2$ then every element in F is a square.
- If $Char(F) \neq 2$ then there are $\frac{q+1}{2}$ squares in F.

We will break the proof into two cases:

Case 1:

Suppose $Char(F) = 2$, and let $a \in F$. We want to find $x, y \in F$ with $x^2+y^2 = a$.

But we know that every element in F is a square. In particular, a is a sqare, so there is an element $b \in F$ with $b^2 = a$. So we can take $x = 0$ and $y = b$ to get:

$$0^2 + b^2 = a$$

Case 2:

Suppose $Char(F) \neq 2$, and let $a \in F$. We want to find $x, y \in F$ with $x^2+y^2 = a$.

Let $S = \left\{b \in F \mid b = c^2, c \in F\right\}$ be the set of squares in F. By the fact above, we know $|S| = \frac{q+1}{2}$.

Let $a - S = \{d \in F \mid d = a - b, b \in S\}$. Since multiplication by -1 and adding a are both bijections, the set $a - S$ is the same size as S. Explicitly, we can define a map:

$$\begin{array}{rcl} \varphi : S & \to & a - S \\ b & \mapsto & a - b \end{array}$$

Suppose $\varphi(b_1) = \varphi(b_2)$. That is, $a - b_1 = a - b_2$. Cancelling a and multiplying by -1 gives $b_1 = b_2$, so this map is injective.

Moreover, given $d \in a - S$ there exists $b \in S$ with $d = a - b$, by the definition of the set $a - S$. This implies that φ is also surjective, so it is a bijection. Thus, S and $a - S$ must have the same size:

$$|a - S| = |S| = \frac{q+1}{2}$$

But these are both subsets of F, and their combined size is greater than the size of F:

$$|a - S| + |S| = \frac{q+1}{2} + \frac{q+1}{2} = q + 1$$

Thus, by the pigeonhole principle, their intersection cannot be empty. That is, we can find an element of F in their intersection:

$$z \in (a - S) \cap S$$

Since $z \in a - S$ it can be written:

$$z = a - x^2$$

for some $x \in F$. However, since $z \in S$ it can be written:

$$z = y^2$$

for some $y \in F$. Thus, we have:

$$z = y^2 = a - x^2$$

In particular, $y^2 = a - x^2$, so we have managed to find $x, y \in F$ satisfying:

$$a = x^2 + y^2$$