Question 1

Let $\mathbb{Z}_3[i] = \{a+bi : a, b \in \mathbb{Z}_3\}$, with addition and multiplication like in the complex numbers but reduced modulo 3. In particular, i^2 is the class of 2 in $\mathbb{Z}_3$. You may assume that $\mathbb{Z}_3[i]$ is a ring under these operations.

(a) Observe that $\mathbb{Z}_3[i]$ has nine elements. Prove that $\mathbb{Z}_3[i]$ is not isomorphic to $\mathbb{Z}_9$. (Hint: if $f : \mathbb{Z}_9 \to \mathbb{Z}_3[i]$ is an homomorphism, consider $f(1)$).

(b) Show that the map $N : \mathbb{Z}_3[i] \to \mathbb{Z}_3$ given by $N(a + bi) = a^2 + b^2$ is well-defined. What is the preimage $N^{-1}(0)$?

(c) Show that $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}_3[i]$. Is N a ring homomorphism?

(d) Find a characterization of invertibility of $x \in \mathbb{Z}_3[i]$ in terms of $N(x)$. Prove your characterizaton.

(e) Show that $\mathbb{Z}_3[i]$ is a field.

Now you know a finite field which is not one of the $\mathbb{Z}_p$. We will see that there is exactly one finite field for every prime power order.