Elementary Explanation of Finite Field Mysteries

By "elementary," I mean using only basic group facts, like the order of an element divides the order of a group, and basic polynomial ring facts, like division algorithm, gcd's, and unique factorization for polynomials with coefficients in any field.

Fact 1 *If $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ is irreducible of degree n, then $f(X)$ has n roots in the field $F = \mathbb{Z}/p\mathbb{Z}[X]/(f(X))$.*

Proof $|F| = q = p^n$, so the multiplicative group F^* has order $|F^*| = q - 1$. Let $x = X \bmod f(X)$. Then $x^{q-1} = 1 \in F^*$. Since $f(X)$ is the minimal polynomial for x, we have $f(X)$ divides $X^{q-1} - 1$ in $\mathbb{Z}/p\mathbb{Z}[X]$ and in $F[X]$. But every element of F^* is a root of $X^{q-1} - 1$, so $X^{q-1} - 1 = \prod(X - a) \in F[X]$, where a ranges over all elements of F^*. Since $f(X)$ divides this product, $f(X)$ has n linear factors in $F[X]$. ∎

Fact 2 *If $g(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ is another irreducible polynomial of degree n, then $g(X)$ has n roots in $F = \mathbb{Z}/p\mathbb{Z}[X]/(f(X))$.*

Proof The proof of Fact 1 shows that $g(X)$ divides $X^{q-1} - 1$ in $\mathbb{Z}/p\mathbb{Z}[X]$ and hence in $F[X]$. But we already factored $X^{q-1} - 1$ in $F[X]$, namely $X^{q-1} - 1 = \prod(X - a) \in F[X]$. So, $g(X)$ is also a product of n linear factors in $F[X]$. ∎

Fact 3 *The fields $F = \mathbb{Z}/p\mathbb{Z}[X]/(f(X))$ and $K = \mathbb{Z}/p\mathbb{Z}[X]/(g(X))$ are isomorphic.*

Proof By Fact 2, $g(X)$ has a root $y \in F$. Thus, there is a copy of K in F. But both have vector space dimension n over $\mathbb{Z}/p\mathbb{Z}$, so $K = F$. ∎

Regarding Statement 1, it is easy enough to make explicit the n roots of $f(X)$ in $F = \mathbb{Z}/p\mathbb{Z}[X]/(f(X))$. Namely, the Frobenius $\sigma(a) = a^p$ is a field automorphism of F which fixes the coefficients of $f(X)$, which are in $\mathbb{Z}/p\mathbb{Z}$. Thus $x, x^p, (x^p)^p, \ldots$ are all roots of $f(X)$. A little Galois theory tells you there is no repetition here until n roots are obtained. That is, the first repetition is $x^q = x$, with $q = p^n$. In somewhat more elementary terms, since x generates F over $\mathbb{Z}/p\mathbb{Z}$, if you had $x^r = x$, with $r = p^d$, $d < n$, then you would have $a^r = a$, for all $a \in F$. This is too many roots for the polynomial $X^r - X$.