A note on zeros of polynomials over $\mathbb{F}_p$.

Proposition. Let $d \in \mathbb{Z}_{>1}$ and p be a prime number. There exist polynomials of degree d over $\mathbb{F}_p$ (more generally, $\mathbb{F}_q$ with $q = p^n$) that have no zeroes in $\mathbb{F}_p$ ($\mathbb{F}_q$).

Proof. We start by observing that the polynomial $x^d - x$ gives a map from $\mathbb{F}_p$ (or $\mathbb{F}_q$) to itself via $\varphi(a) = a^d - a$ $\forall a \in \mathbb{F}_p$ with $\varphi(0) = 0^d - 0 = 0$ and $\varphi(1) = 1^d - 1 = 0$. As φ is a map from a finite set to itself, which is not one-to-one (injective), it is not onto (surjective) either. Therefore, there exists an element $a \in \mathbb{F}_p$, not in the image of φ. In other words, $\varphi(x) = x^d - x \not\equiv a$ $\forall x \in \mathbb{F}_p$, hence, the polynomial $g(x) := x^d - x - a$ has no zeros in $\mathbb{F}_p$.

Example. Let $d = 5$ and $p = 3$, we compute the values of $\varphi(x) = x^5 - x$: $\varphi(0) = \varphi(1) = 0$ and $\varphi(2) = 2^5 - 2 = 30 \equiv 0$. This allows to conclude (as both 1 and 2 are 'missed' by φ) that the polynomials $x^5 - x - 1$ and $x^5 - x - 2$ have no zeros over $\mathbb{F}_3$. Indeed, we check that $x^5 - x - 1 \equiv 2$ and $x^5 - x - 2 \equiv 1$ over $\mathbb{F}_3$.

Observation. Notice that a polynomial of degree d can not have exactly $d-1$ zeros over a field $\mathbb{k}$. This follows from the fact that the sum of all d zeros of a polynomial is equal to $-a_{d-1}$ (the coefficient of x^{d-1}), which is in $\mathbb{k}$.

In particular, a polynomial of degree 3 can have 0, 1 or 3 zeros over a finite field $\mathbb{k}$ and 1 or 3 zeros over real numbers.

Recall that for an elliptic curve given by equation $y^2 = f(x)$ (a polynomial of degree 3 without multiple zeros) the number of points of order 2 in the corresponding group is equal to the number of zeros of $f(x)$. More precisely, these points are $\{(a, 0) \mid f(a) = 0\}$.