Polynomial Fundamentals:

1. We define polynomials by the values they return at each input. $P(0) = 4$ for example returns the value 4 for input $x = 0$. Two polynomials g, f are identical if they return same values for all inputs: $\forall x(f(x) = g(x)$, and they are distinct if they return any different values for same input: $(\exists x)(f(x) \neq g(x)$.

2. Degree d of a polynomial $P(x)$ is the degree of its largest exponent of x with non-zero coefficient. Thus, a polynomial of degree d, can be represented as:

$$P(x) = a_d x^d + a_{d-1} x^{d-1}. + ... + a_1 x^1 + a_0$$

3. We can uniquely identify a polynomial of degree d using:

   (a) any d+1 points on the polynomial (arbitrary points on the polynomial still works)

   (b) the specific d+1 coefficients of the polynomial: ax + b has coefficients a, b and every different combination of a and b values define a different polynomial of degree 1. Above, the polynomial P(x) has d+1 coefficients $a_d, a_{d-1}, ...a_1, a_0$

4. In order to use given points to get to the polynomial we use Lagrange interpolation (see section below). In order for Lagrange interpolation to give the correct P(x), the number of points included in interpolation should be d+1 as mentioned. Any number of points less than this will give an equation that can be fit to multiple polynomials based on the values of the remaining required points for uniqueness.

5. Roots of a polynomial are points where the polynomial intersects the x axis. At a polynomial's root, $P(x*) = 0$ such that $x*$ are x-coordinates of x-axis intercepts. Not all polynomials have to have a root ($g(x) = x^2 + 1$ for example has no roots). A degree d polynomial can have at most d roots.

6. A zero polynomial is a polynomial has infinite roots, and is defined as

$$\forall x f(x) = 0$$

7. Adding together polynomials doesn't increase the number of roots over individual f or g's roots. The maximum number of roots of f + g is max(degree f, degree g). If neither f or g has roots, then f+g also have no roots. One exception is when f = -g, and f+g is a zero polynomial, which has infinite roots.

8. Multiplying together polynomials however increases number of roots of (f g) since any root of f is a root of f g and any root of g is a root of f g as well. So the maximum possible number of roots would be (degree f) +(degree g) and minimum number of roots would again be 0 if neither f or g has any roots to contribute.

9. If $P(x)$ is a nonzero polynomial and a is root of P. Then $P(x)$ can be written as $(x - a)Q(x)$ where Q is a non zero polynomial of degree one less than that of P. Remember if we know all d roots r_i of $P(x)$, we can represent the polynomial as $P(x) = (x - r_1)(x - r_2)..(x - r_{d+1})$

Polynomials in GF(p): Wrapping up Polynomials

1. Polynomials under $GF(p)$ have restricted options for values each input can take. In $GF(p)$, $P(x)$ can only take values $(0, 1, 2, \ldots, p-1)$. $GF(p)$ offers p distinct values per each x input of the polynomial.

2. Under $GF(p)$, the maximum degree of a polynomial is $p-1$. $GF(p)$ can only offer p distinct x values we can only uniquely define polynomials of degree (p-1) in $GF(p)$. Any polynomials with degree larger than p-1 cannot be uniquely determined in $GF(p)$.

3. Since we know each point can get p different values in $GF(p)$, we can show the relationship between #known points on the polynomial of degree d and #unique polynomials in GF(p) as in the table below:

#known/fixed points on the polynomial	#different polynomials
d+1	1
d	p
d-1	p^2
…	…
k	p^(d+1-k)
…	…
1	p^d
0	p^(d+1)

Figure 1: Number of unique polynomials of degree d with varying fixed points in $GF(p)$

Lagrange Interpolation: Points $(x_i, y_i) \Longrightarrow$ Polynomial $P(x)$

1. Lagrange Interpolation process gives a polynomial that crosses through all the points inputted in calculation. Therefore, even though we need d+1 to uniquely define a polynomial, we can get more general polynomial descriptions for less points, that'd fit more than one polynomial.

2. The process is simple: Given $(x_0, y_0), (x_1, y_1), (x_2, y_2), ..., (x_d, y_d)$: i) First, calculate polynomials corresponding to each pair represented as: $\Delta_0, \Delta_1, ..., \Delta_d$ and then combine individual polynomials Δ_i with their corresponding y_i as coefficients to interpolate $P(x)$ as:

$$P(x) = \sum_{i=0}^{d} y_i \Delta_i \text{ where } \Delta_i = \frac{\prod_{i \neq j}(x - x_j)}{\prod_{i \neq j}(x_i - x_j}$$

3. Remember that in GF(p), while calculating Δ_i for each point, use modular arithmetic rules of using multiplicative inverses instead of division in order to handle the denominators.