Exercise 1

(a) Determine the order of $(x^2 + x + 1)^5(x^3 + x + 1)$ over $\mathbb{F}_2$.
(b) Determine the order of $x^7 - x^6 + x^4 - x^2 + x$ over $\mathbb{F}_3$.

Exercise 2

(a) $\text{ord}(Q_e) = e$ for all $e$ for which the cyclotomic polynomial $Q_e \in \mathbb{F}_q[x]$ is defined.
(b) Let $f$ be irreducible over $\mathbb{F}_q$ with $f(0) \neq 0$, and let $e \in \mathbb{N}$ be relatively prime to $q$. Then $\text{ord}(f) = e$ if and only if $f$ divides the cyclotomic polynomial $Q_e$.

Exercise 3

For $m \in \mathbb{N}$, let $\phi(m) = |\{k \in \mathbb{N} \mid 1 \leq k \leq m, \gcd(k, m) = 1\}|$. For $m, n, s \in \mathbb{N}$ and $p$ prime, show

(a) $\phi(p^s) = p^s(1 - 1/p)$
(b) $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$
(c) $\phi(m) = m(1 - 1/p_1) \cdots (1 - 1/p_r)$ where $m = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of $m$.

Calculate $\phi(490)$ and $\phi(768)$.

Exercise 4

Let $\mathbb{F}_q$ be a finite field of characteristic $p$, and let $f \in \mathbb{F}_q[x]$ be a polynomial of positive degree with $f(0) \neq 0$. Then $\text{ord}(f(x^p)) = p\text{ord}(f(x))$. 