Finite Fields: Multiplicative Structure
Notation: Henceforth, let $F$ denote the finite field $GF(p^m)$ and let $F^* = F \setminus \{0\}$ be the set of nonzero elements in $F$.

Definition: Multiplicative order of field elements

For every $\alpha \in F^*$, the multiplicative order of $\alpha$ is the smallest positive integer $r$ such that $\alpha^r = 1$. That is

$$o(\alpha) \overset{\text{def}}{=} \min\{r > 0 : \alpha^r = 1\}$$

- Order of $\alpha$ always exists since $F^*$ is finite. The sequence $1, \alpha, \alpha^2, \ldots$ cannot keep generating distinct elements forever. Thus there must be a repetition $\alpha^j = \alpha^i$ for some $i < j$, and then $\alpha^{j-i} = 1$.

- The powers $1, \alpha, \alpha^2, \ldots, \alpha^{o(\alpha)-1}$ are all distinct. Otherwise, if $\alpha^j = \alpha^i$ for some $0 \leq i < j < o(\alpha)$ then $\alpha^{j-i} = 1$ and $o(\alpha)$ is not minimal.
Properties of multiplicative order

Lemma 1: Divisibility by the order

\[ \alpha^s = 1 \iff o(\alpha) \mid s \]

Lemma 2: Order of a power

\[ o(\alpha^i) = \frac{o(\alpha)}{\gcd(i, o(\alpha))} \]

Lemma 3: Order of a product

If \( o(\alpha) \) and \( o(\beta) \) are relatively prime, then \( o(\alpha \beta) = o(\alpha) o(\beta) \).

These lemmas are increasingly difficult to prove. We will prove the first lemma, leaving the other two for extra-credit on the homework.
Lemma 1: Divisibility by the order

\[ \alpha^s = 1 \iff o(\alpha) \mid s \]

**Proof.**

- \((\Leftarrow)\) If \(s = t \cdot o(\alpha)\), then \(\alpha^s = \alpha^{t \cdot o(\alpha)} = \left(\alpha^{o(\alpha)}\right)^t = 1^t = 1\)

- \((\Rightarrow)\) Write \(s = q \cdot o(\alpha) + r\) with \(r < o(\alpha)\). Then

  \[ 1 = \alpha^s = \alpha^{q \cdot o(\alpha)} \alpha^r = \left(\alpha^{o(\alpha)}\right)^q \alpha^r = \alpha^r \]

  This implies that \(r = 0\). Otherwise \(\alpha^r = 1\) would contradict the minimality of \(o(\alpha)\), since \(r < o(\alpha)\).
Primitive element: The main theorem

Definition: Primitive element of a field
An $\alpha \in F^*$ is a **primitive element** if $o(\alpha) = |F^*| = p^m - 1$. Equivalently

$$F = \{ 0, \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{p^m-2} \}$$

Theorem: Multiplicative structure of finite fields

*Every finite field contains a primitive element.*

**Proof.** Take $\alpha$ to be the element of the highest order in the field. That is $o(\alpha) \geq o(\beta)$ for all $\beta \in F^*$. We claim that

$$o(\beta) \text{ divides } o(\alpha) \text{ for all } \beta \in F^*$$

To prove the claim, consider any prime divisor $q$ of $o(\beta)$. Divide $q$ into $o(\beta)$ and $o(\alpha)$ to write $o(\beta) = q^b \cdot s$ with $q \nmid s$ and $o(\alpha) = q^a \cdot t$ with $q \nmid t$. 
Proof of the claim

Now let $\gamma = \alpha^{q^a}$. Then

$$o(\gamma) = \frac{o(\alpha)}{\gcd(q^a, o(\alpha))} = \frac{o(\alpha)}{q^a} = t$$

Also

$$o(\beta^s) = \frac{o(\beta)}{\gcd(s, o(\beta))} = \frac{o(\beta)}{s} = q^b$$

Since $o(\gamma) = t$ and $o(\beta^s) = q^b$ are relatively prime, it now follows from Lemma 3 that $o(\gamma \cdot \beta^s) = q^b t$. Since $o(\alpha) = q^a t$ is maximal in the field

$$q^b \cdot t \leq q^a \cdot t \implies b \leq a \implies q^b | o(\alpha)$$

This is true for any prime divisor of $o(\beta)$. Since we can decompose $o(\beta)$ as a product of powers of its prime divisors, $o(\beta)$ divides $o(\alpha)$. 
Proof of the main theorem

Let \( r = o(\alpha) \). We can now conclude:

\[
o(\beta) \text{ divides } r \text{ for all } \beta \in \mathbb{F}^* \\
\Downarrow \\
\beta^r = 1 \text{ for all } \beta \in \mathbb{F}^* \\
\Downarrow \\
\beta \text{ is a zero of the polynomial } x^r - 1, \text{ for all } \beta \in \mathbb{F}^*
\]

It follows that the polynomial \( f(x) = x^r - 1 \) has at least \( |\mathbb{F}^*| = p^m - 1 \) different roots. Consequently, \( \text{deg } f(x) = r \) must be at least \( p^m - 1 \).

But \( \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{r-1} \) are distinct, and there are at most \( |\mathbb{F}^*| = p^m - 1 \) distinct nonzero elements in \( \mathbb{F} \). This implies that

\[
o(\alpha) = r = p^m - 1
\]
Factorization of the $x^{p^m} - x$ polynomial

It follows from the proof of the main theorem that every $\beta \in \text{GF}(p^m)$ satisfies the equation

$$x \left( x^{p^m-1} - 1 \right) = x^{p^m} - x = 0$$

The polynomial $x^{p^m} - x$ has degree $p^m$, and we have identified $p^m$ different zeros of this polynomial in $\text{GF}(p^m)$. Every such zero corresponds to a different linear factor of $x^{p^m} - x$. Thus

$$x^{p^m} - x = \prod_{\beta \in \text{GF}(p^m)} (x - \beta)$$

Observe that the right-hand side is computed in $\text{GF}(p^m)$, but produces only 0, +1, and −1 coefficients.
Theorem: Exponentiation in fields of characteristic $p$

In a field of characteristic $p$, we have

\[(x + y)^p = x^p + y^p\]

**Proof.** By the binomial theorem:

\[(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = \binom{p}{0} x^0 y^p + \binom{p}{p} x^p y^0 = x^p + y^p\]

since for $k = 1, 2, \ldots, p - 1$, we have

\[\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k} \equiv 0 \mod p\]
Exponentiation as a linear operation

Corollary: Exponentiation in fields of characteristic $p$

In a field of characteristic $p$, we have

$$(x + y)^{p^i} = x^{p^i} + y^{p^i}$$

Proof. Apply the foregoing theorem $i$ times. For example

$$(x + y)^{p^2} = ((x + y)^p)^p = (x^p + y^p)^p = (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}$$