Highlights of Chapters 8 and 10.

Chapter 8: Primitive Roots

1. Definition of order mod m: the multiplicative order of a unit a mod m is the least natural number $n \geq 1$ such that $a^n \equiv 1 \bmod m$.
2. If $a^t \equiv 1 \bmod m$, then $\mathrm{ord}_m\, a$ divides t. In particular,
   - The order of a unit modulo p, a prime, always divides $p - 1$.
   - The order of a unit modulo m always divides $\varphi(m)$.
3. The order of a^d mod m is given by $\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a),d)}$.
4. If $\mathrm{ord}_m(a) = h$ and $\mathrm{ord}_m(b) = k$, and $\gcd(h, k) = 1$, then $\mathrm{ord}_m(ab) = hk$.
5. Definition of primitive root: g mod m is a primitive root if $\mathrm{ord}_m(g) = \varphi(m)$.
6. Lemma: if g mod m is a primitive root, then $\{g, g^2, \ldots, g^{\varphi(m)} \bmod m\}$ is are all the units mod m.
7. If $\mathbb{Z}/m\mathbb{Z}$ has at least one primitive root, then there are exactly $\varphi(\varphi(m))$ primitive roots.
8. Theorem: for every prime p there is at least one primitive root in $\mathbb{Z}/p\mathbb{Z}$.

Chapter 10: Quadratic Congruences

1. To solve $ax^2 + bx + c \equiv 0 \bmod m$, the quadratic formula $x \equiv \frac{-b+s}{2a} \bmod m$ works as long as $\gcd(2a, m) = 1$, where s is any root of $x^2 \equiv b^2 - 4ac \bmod m$.
2. Definition of quadratic residue and quadratic non-residue: a unit a mod m is a QR if there is some b mod m such that $b^2 \equiv a \bmod m$. The class of a is a QNR if there is no b such that $b^2 \equiv a \bmod m$.
3. Theorem: for any prime $p > 2$, the class of -1 is a QR if and only if $p \equiv 1 \bmod 4$.
4. Definition of the Legendre symbol, for p a prime: $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a QR}, \\ -1 & \text{if } a \text{ is a QNR.} \end{cases}$
5. Properties of the Legendre symbol, for a prime p and any $a, b \in \mathbb{Z}$:
   - $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \bmod p$,
   - $\left(\frac{a}{p}\right) = \left(\frac{ab^2}{p}\right)$, and $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
   - $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, and $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
   - Euler's criterion: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.
6. Law of Quadratic Reciprocity: if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \text{ or } q \equiv 1 \bmod 4, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$