Highlights of Chapters 4,5,7,8.

Chapter 4: Congruences

1. Definition of congruence: $a \equiv b \bmod m$ if $m|a-b$.
2. Properties of congruences, e.g., if $a \equiv b \bmod m$, then $a^k \equiv b^k \bmod m$, for all $k \geq 1$.
3. Cancellation properties of congruences, e.g., if $ac \equiv bc \bmod m$, then $a \equiv b \bmod \frac{m}{\gcd(m,c)}$.
4. The congruence $ax \equiv b \bmod m$ has a solution if and only if $ax + my = b$ has a solution $x, y \in \mathbb{Z}$, if and only if $\gcd(a, m)$ divides b.
5. Systems of congruences: the Chinese remainder theorem. If $\gcd(m, n) = 1$, then the system $\{x \equiv a \bmod m,\ x \equiv b \bmod n\}$ has a unique solution modulo mn, for any integers $a, b \in \mathbb{Z}$.
6. Applications of congruences: Divisibility tests, e.g., a number is divisible by 9 if the sum of digits is divisible by 9; check digits.

Chapter 5: Groups, rings and fields

1. Definition of congruence classes and the set $\mathbb{Z}/m\mathbb{Z}$.
2. Definition of group, ring, field.
3. Definition of unit (multiplicative inverse), zero-divisor.
4. A congruence $a \bmod m$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ if $\gcd(a, m) = 1$; a zero-divisor if $\gcd(a, m) > 1$.
5. $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.
6. A polynomial of degree n over $\mathbb{Z}/p\mathbb{Z}$ has at most n roots modulo p, even when counted with multiplicities.

Chapter 7: The theorems of Wilson, Fermat and Euler

1. Wilson's theorem: A number p is prime if and only if $(p-1)! \equiv -1 \bmod p$.
2. Fermat's Last Theorem: the equation $x^n + y^n = z^n$ has no integral solutions when $xyz \neq 0$ and $n > 3$.
3. Fermat's little theorem:
   - If p is a prime, then $n^p \equiv n \bmod p$, for all n.
   - (Alternative statement) If p is prime, then $a^{p-1} \equiv 1 \bmod p$ whenever $\gcd(a, p) = 1$.
4. Euler's phi function: $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$.
5. Euler's theorem: $a^{\varphi(m)} \equiv 1 \bmod m$ whenever $\gcd(a, m) = 1$.
6. Properties of Euler's phi function:
   - If p is a prime, then $\varphi(p) = p - 1$.
   - If p is a prime and $n \geq 1$, then $\varphi(p^n) = p^{n-1}(p-1)$.
   - If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.
7. If $\gcd(m, n) = 1$, then there is a bijection $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ that sends $a \bmod mn$ to $(a \bmod m, a \bmod n)$. This bijection sends units to units.

Chapter 8: Order and Primitive Roots

1. Definition of order mod m: the multiplicative order of a unit $a \bmod m$ 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 $\operatorname{ord}_m a$ 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. (Chapter to be continued...)