Highlights of Chapters 1-4.

Chapter 2: The Integers $\mathbb{Z}$

1. Well ordering principle of $\mathbb{N}$: every non-empty set of $\mathbb{N}$ has a least element.
2. Principle of Mathematical Induction: If (a) the statement is true for n_0, and (b) if the statement is true for k, this implies $k+1$ is true, then the statement is true for all $n \geq n_0$.
3. Division Theorem: $a, b \in \mathbb{Z}$, $b \neq 0$, then there are $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.
4. Definition of divisibility: $b|a$ if there is $k \in \mathbb{Z}$ such that $a = bk$.
5. Greatest common divisor: $d = \gcd(a, b)$ if (a) $d|a$ and $d|b$, and (b) if $e|a$, $e|b$ then $e \leq d$.
6. Euclid's algorithm (based on repeated long division).
7. Bezout's identity: $ax + by = c$ has solutions $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b)|c$.
   (a) Rational roots of polynomials.
   (b) Points in a line: if (x_0, y_0) is one solution for $ax + by = c$, then all the solutions are given by $x = x_0 + \frac{bk}{d}$, $y = y_0 - \frac{ak}{d}$, for all $k \in \mathbb{Z}$, where $d = \gcd(a, b)$.
8. Key corollary of Bezout's identity, Euclid's Lemma: if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.
9. Fundamental theorem of arithmetic
   (a) Every number has a factorization as a product of primes $n = p_1^{e_1} \cdots p_t^{e_t}$, where $p_1 < p_2 < \cdots < p_t$ are primes and $e_t \geq 1$.
   (b) The factorization into primes is unique up to a reordering of prime-power factors.

Chapter 3: The Prime Numbers

1. The sieve of Eratosthenes.
2. Euclid's theorem on the infinitude of the primes: if $S = \{p_1, \ldots, p_n\}$ are primes, then $N = p_1 p_2 \cdots p_n + 1$ is divisible only by (new) primes not in the set S.
3. Bertrand's postulate: for all $n \geq 2$ there is a prime $n < p < 2n$.
4. The prime number theorem: $\pi(x)$ is approximately $x/\log x$ for large x.
5. Dirichlet's theorem on primes in arithmetic progressions: if $\gcd(a, m) = 1$, then there are infinitely many primes $p \equiv a \bmod m$.
6. The twin prime conjecture: there are infinitely many primes p such that $p + 2$ is also prime.
7. Goldbach's conjecture: every even number $n > 2$ can be written $n = p + q$, with p, q primes.

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.
   (a) Divisibility tests, e.g., a number is divisible by 9 if the sum of digits is divisible by 9.
   (b) Check digits.