1.1: Section 1.1
   (a) Def: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
   (b) Def: $S \subseteq \mathbb{R}$ is well-ordered if every subset has a least element.
   (c) Thm: $\mathbb{Z}^+$ is well-ordered.
   (d) Def: $\alpha \in \mathbb{R}$ is algebraic if it is the root of a polynomial with integer coefficients. Otherwise it is transcendental.
   (e) Def: $S$ is countable if it is finite or if there is a 1-1 correspondance between $S$ and $\mathbb{Z}^+$. Otherwise it is uncountable.

1.2: (a) Def: Of the sum $\Sigma$.
(b) Def: Of the product $\Pi$.

1.3: (a) Thm: If $S \subseteq \mathbb{Z}^+$ is such that $1 \in S$ and if $k \in S$ then $k + 1 \in S$, then $S = \mathbb{Z}^+$.
(b) Thm: If $S \subseteq \mathbb{Z}^+$ is such that $1 \in S$ and if $1, \ldots, k \in S$ then $k + 1 \in S$ then $S = \mathbb{Z}^+$.

1.5: (a) Def: We have $a \mid b$ if $\exists c \in \mathbb{Z}$ with $ac = b$.
(b) Thm: If $a \mid b$ and $b \mid c$ then $a \mid c$.
(c) Thm: If $a, b \in \mathbb{Z}$ with $b > 0$ then $\exists q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.
(d) Def: $\gcd(a, b)$ is the largest integer dividing both $a$ and $b$.
(e) Def: $a, b$ are coprime if $\gcd(a, b) = 1$.

3.1: (a) Def: $a \in \mathbb{Z}$ with $a > 1$ is prime if its only divisors are 1 and itself. Otherwise it is composite.
(b) Thm: There are infinitely many primes.
(c) Thm: If $n$ is composite then it has a prime factor less than or equal to $\sqrt{n}$.

3.2: (a) Def: $\pi(x)$ is the number of primes less than or equal to $x \in \mathbb{R}^+$.
(b) Thm: We have $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$.
(c) Thm: For large $x$ we have $\pi(x) \approx x/\ln x$.
(d) Def: $p_n$ denotes the $n^{th}$ prime.
(e) Thm: We have $\lim_{n \to \infty} \frac{p_n}{n \ln n} = 1$.
(f) Thm: For large $n$ we have $p_n \approx n \ln n$.
(g) Thm: For any $n$ we can find $n$ consecutive composites.

3.3: (a) Thm: For $a, b \in \mathbb{Z}$ we have $\gcd(a, \gcd(a, b), b/\gcd(a, b)) = 1$.
(b) Thm: We have $\gcd(a, b) = \gcd(a, b + ka)$.
(c) Thm: $\gcd(a, b)$ is the smallest positive linear combination of $a, b$.
(d) Thm: If $a, b$ are coprime then there are $x, y$ with $ax + by = 1$.
(e) Thm: The set of linear combinations of $a, b$ equals the set of multiples of $\gcd(a, b)$.
(f) Thm: $d = \gcd(a, b)$ iff we have $d \mid a$ and $d \mid b$ and if $c \mid a$ and $c \mid b$ then $c \mid d$.

3.4: (a) Thm: The Euclidean Algorithm gives us $\gcd(a, b)$.
(b) Thm: The process of the EA calculation can give us the linear combination which yields $\gcd(a, b)$.
3.5: (a) **Thm:** Every positive integer greater than 1 can be written uniquely as a product of powers of primes. This the prime factorization (PF) of the integer.

(b) **Thm:** If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

(c) **Thm:** If a prime $p \mid a_1 \ldots a_n$ then $p \mid a_i$ for some $i$.

(d) **Thm:** $a \mid b$ iff whenever $p^k$ appears in the PF of $a$ then $p^j$ appears in the PF of $b$ with $j \geq k$.

(e) **Thm:** The positive divisors of $n$ are those integers whose prime power factorizations have the same primes as $n$ with powers less than or equal to those powers occurring in $n$.

(f) **Thm:** The greatest common divisor of two integers equals the integer whose prime power factorization contains primes common to both prime power factorizations each with a power equal to the minimum power occurring in those two.

(g) **Thm:** The least common multiple of two integers equals the integer whose prime power factorization contains primes occurring in either prime power factorization each with a power equal to the maximum power occurring in those two.

(h) **Thm:** For integers $a, b$ not both zero we have $ab = \gcd(a, b)\text{lcm}(a, b)$.

(i) **Thm:** Suppose $n_1, n_2 \in \mathbb{Z}$ with $\gcd(n_1, n_2) = 1$. Suppose $d \mid n_1 n_2$. Then $d = d_1 d_2$ with $\gcd(d_1, d_2) = 1$ and $d_1 \mid n_1$ and $d_2 \mid n_2$.

4.1: (a) **Def:** $a \equiv b \mod m$ if $m \mid (a - b)$.

(b) **Thm:** $a \equiv b \mod m$ iff $\exists k \in \mathbb{Z}$ with $a + km = b$.

(c) **Thm:** If $ac \equiv bc \mod m$ then $a \equiv b \mod \gcd(m, c)$.

(d) **Def:** Given a modulus $m$ the integers are divided into $m$ distinct congruence classes mod $m$.

(e) **Def:** A complete set of residues mod $m$ is a set of $m$ integers, one from each class.

(f) **Thm:** If a set of $m$ integers has the property that no two are congruent mod $m$ then they form a complete set of residues.

(g) **Def:** The set $\{0, 1, \ldots, m - 1\}$ is the complete set of least nonnegative residues mod $m$.

(h) **Thm:** If $\{r_1, r_2, \ldots, r_m\}$ is a complete set of residues and if $a, b \in \mathbb{Z}$ with $\gcd(a, m) = 1$ then $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ is a complete set of residues.

(i) **Calc:** Fast exponentiation.

4.2: (a) **Thm:** The linear congruence $ax \equiv b \mod m$ has solutions iff $\gcd(m, a) \mid b$ and if so then it has $\gcd(m, a)$ solutions which are incongruent to one another mod $m$ and if $x_0$ is one of them then all are $x = x_0 + km/\gcd(m, a)$ for $k = 0, 1, \ldots, \gcd(m, a) - 1$.

4.3: (a) **Thm:** If $m_1, \ldots, m_r$ are pairwise coprime then the system $x \equiv a_i \mod m_i$ for $i = 1, \ldots, r$ has a unique solution mod $M = m_1 \ldots m_r$ given by $x = a_1 M_1 y_1 + \ldots + a_r M_r y_r$ where $M_i = M/m_i$ and $M_i y_i \equiv 1 \mod m_i$.

4.6: (a) **Thm:** If $n$ has a small factor $p$ then a divisor of $n$ may often be quickly found by assigning $x_0 = 2$ (usually) and $x_1 = x_0^2 + 1 \mod n$, $x_2 = x_1^2 + 1 \mod n$, and so on, and then by progressively testing $\gcd(x_{2s} - x_s, n)$ whenever possible. If a value other than 1 arises then that is a factor.