Hints to Homework Set 2
(Homework Problems from Chapter 1)

Problems from Section 1.1.
1.1.1. Let \( n \) be an integer. Prove that \( a \) and \( c \) leave the same remainder when divided by \( n \) if and only if \( a - c = nk \) for some \( k \in \mathbb{Z} \).

- \( \implies \) Apply Division Algorithm to \( a \) and \( c \)

\[
\begin{align*}
a &= q_1n + r_1 \\
c &= q_2n + r_2
\end{align*}
\]

and subtract.

- \( \iff \) Suppose \( a - c = nk \). The Division algorithm says we can find integers \( q_1, r_1, q_2, r_2 \) such that

\[
\begin{align*}
a &= q_1n + r_1 \quad \text{with } 0 \leq r_1 < n \\
c &= q_2n + r_2 \quad \text{with } 0 \leq r_2 < n
\end{align*}
\]

We thus have

\[
 nk = a - c = q_1n + r_1 - (q_2n + r_2) = n(q_1 - q_2) + r_1 - r_2
\]

or

\[
 r_1 - r_2 = (k - q_1 - q_2)n
\]

Thus, \( n \mid (r_1 - r_2) \). Now note that \( 0 \leq |r_1 - r_2| < n \) (this follows from \( 0 \leq r_1 < n \) and \( 0 \leq r_2 < n \)). But the only non-negative integer smaller than \( n \) that is divisible by \( n \) is 0. So we must have

\[
 r_1 - r_2 = 0 \implies r_1 = r_2.
\]

1.1.2. Let \( a \) and \( c \) be integers with \( c \neq 0 \). Then there exist unique integers \( q \) and \( r \) such that

- \( a = cq + r \)
- \( 0 \leq r < |c| \).

- If \( c > 0 \), then this is just the Division Algorithm theorem. If \( c < 0 \), then the Division Algorithm theorem can be applied to \( -c = |c| \).

\[
\exists ! \ q, r \in \mathbb{Z} \ s.t. \ a = |c|q + r \quad \text{with } 0 \leq r < |c|
\]

Now write

\[
a = (-c)(-q) + r
\]

1.1.3. Prove that the square of any integer \( a \) is either of the form \( 3k \) or of the form \( 3k + 1 \) for some integer \( k \).

- There possibilities for \( n \) can be split into three subcases.

\[
\begin{align*}
n &= 3q \\
n &= 3q + 1 \\
n &= 3q + 2
\end{align*}
\]

- Examine the form of \( n^2 \) in each of these cases.

1.1.4. Prove that the cube of any integer has exactly one of the forms \( 9k \), \( 9k + 1 \), or \( 9k + 8 \).

- Use the same technique as the preceding problem.

Problems from Section 1.2
1.2.1. (a) Prove that if \( a \mid b \) and \( a \mid c \) then \( a \mid (b + c) \).

- Simply write \( b = as \) and \( c = at \) and consider the sum \( b + c = as + at \)

(b) Prove that if \( a \mid b \) and \( a \mid c \), then \( a \mid (br + ct) \) for any \( r, t \in \mathbb{Z} \).
• Use same technique as above

1.2.2. Prove or disprove that if $a \mid (b + c)$, then $a \mid b$ or $a \mid c$.

• Find a counter-example

1.2.3. Prove that if $r \in \mathbb{Z}$ is a non-zero solution of $x^2 + ax + b = 0$ (where $a, b \in \mathbb{Z}$), then $r \mid b$.

• Just note that if $r$ satisfies $x^2 + ax + b = 0$, then $b = -r^2 - ar$

1.2.4. Prove that $GCD(a, a + b) = d$ if and only if $GCD(a, b) = d$.

• Show that the sets

\[
S = \{\text{common divisors of } a \text{ and } a + b \} \\
T = \{\text{common divisors of } a \text{ and } b \}
\]

coincide.

1.2.5. Prove that if $GCD(a, c) = 1$ and $GCD(b, c) = 1$, then $GCD(ab, c) = 1$.

• Use the Theorem stating $GCD(a, c) = ua + vc$ for some $u, v \in \mathbb{Z}$ to conclude that there exists $u, v \in \mathbb{Z}$ such that

\[
1 = ua + vc \\ b = bua + bvc = (ba) a + (bv) c
\]

and so anything that divides both $(ba)$ and $c$ will divide $b$. So the greatest common divisor of $ba$ and $c$ must be less than or equal to the greatest common divisor of $b$ and $c$.

1.2.6. (a) Prove that if $a, b, u, v \in \mathbb{Z}$ are such that $au + bv = 1$, then $GCD(a, b) = 1$.

Suppose $a, b$ have a common divisor $t > 1$. Then

\[
1 = au + bv = (xt) u + (yt) v = t(xu + yv)
\]

But then $t\mid 1$ and $|t| > 1 \Rightarrow \text{contradiction!}$

(b) Show by example that if $au + bv = d > 0$, then $GCD(a, b)$ need not be $d$.

Problems from Section 1.3

1.3.1. Let $p$ be an integer other than $0, \pm 1$. Prove that $p$ is prime if and only if for each $a \in \mathbb{Z}$, either $GCD(a, p) = 1$ or $p \mid a$.

• $\Rightarrow$ If $p$ is prime then since its only divisors are $\{-1, -|p|, +1, |p|\}$ its greatest common divisor with any number must be either $1$ or $|p|$. So either $GCD(a, p) = 1$, or $GCD(a, p) = |p|$. In the latter case, $|p|$ is a divisor of $a$, hence so is $p$.

• $\Leftarrow$ Suppose $p \neq 0, \pm 1$ has the property that for any $a \in \mathbb{Z}$ either $GCD(a, p) = 1$ or $p|a$. Suppose $p$ has a non-trivial factorization $p = rs$, $1 < |r| |s| < |p|$

Then since $r \in \mathbb{Z}$, either $1 = GCD(r, p) = r$ or $p|r$ which requires $|p| \leq |r|$.

1.3.2 Let $p$ be an integer other than $0, \pm 1$ with this property: Whenever $b$ and $c$ are integers such that $p \mid bc$, then $p \mid c$ or $p \mid b$. Prove that $p$ is prime.

• Suppose $p$ has a non-trivial factorization $p = rs$ and note the contradiction that arises since $p|p \Rightarrow p|rs$ (which will be similar to the second part of Problem 1.3.1).
1.3.3. Prove that if every integer integer $n > 1$ can be written in one and only one way in the form

$$n = p_1 p_2 \cdots p_r$$

where the $p_i$ are positive primes such that $p_1 \leq p_2 \leq \cdots \leq p_r$.

1.3.4. Prove that if $p$ is prime and $p \mid a^n$, then $p^n \mid a^n$.

1.3.5.
(a) Prove that there exist no nonzero integers $a, b$ such that $a^2 = 2b^2$.

- Show that the two sides of $a^2 = 2b^2$ can not have the same number of prime factors, and so they can’t be equal.

(b) Prove that $\sqrt{2}$ is irrational.

- If

$$\sqrt{2} = \frac{a}{b}, \quad a, b \in \mathbb{Z}$$

then

$$a^2 = 2b^2$$

and apply Part (a) to furnish a contradiction.