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 $k \in \mathbb{Z}$.

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

(i) $a = cq + r$
(ii) $0 \leq r < |c|$

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 $k$.

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

Problems from Section 1.2

1.2.1. (a) Prove that if $a | b$ and $a | c$ then $a | (b + c)$.
(b) Prove that if $a | b$ and $a | c$, then $a | (br + ct)$ for any $r, t \in \mathbb{Z}$.

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

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 $r | b$.

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

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

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

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

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 $p | a^n$, then $p^n | a^n$.

1.3.5. (a) Prove that there exist no nonzero integers $a, b$ such that $a^2 = 2b^2$.
(b) Prove that $\sqrt{2}$ is irrational.