Chapter 4

Question 1. Let $a, b \in \mathbb{Z}$. Show that $4 \mid a^2 - b^2$ iff a and b have the same parity.

Proof. Assume that $4 \mid a^2 - b^2$, then $a^2 - b^2 = 4n$ for some $n \in \mathbb{Z}$, so $(a+b)(a-b) = 4n$. If a and b had opposite parity, then both $(a+b)$ and $(a-b)$ would be odd, and so $(a+b)(a-b)$ would also be odd. However, $4n = 2(2n)$, and since $2n \in \mathbb{Z}$, $4n$ is even. We conclude that a and b must have the same parity.

Conversely, assume that a and b have the same parity.

Case 1: a and b are even. Then $a = 2n$ and $b = 2m$ for some $n, m \in \mathbb{Z}$. So $a^2 - b^2 = 4n^2 - 4m^2 = 4(n^2 - m^2)$. Since $n^2 - m^2 \in \mathbb{Z}$, $4 \mid a^2 - b^2$.

Case 2: Now assume both a and b are odd. Then $a = 2n+1$ and $b = 2m+1$ for some $n, m \in \mathbb{Z}$. So $a^2 - b^2 = (2n+1)^2 - (2m+1)^2 = (4n^2 + 4n + 1) - (4m^2 + 4m + 1) = 4n^2 + 4n - 4m^2 - 4m = 4(n^2 + n - m^2 - m)$. Now $\mathbb{Z}$ is closed under multiplication and addition, so $n^2 + n - m^2 - m \in \mathbb{Z}$ if $n, m \in \mathbb{Z}$. This means we can write $a^2 - b^2$ in the form $4k$ where $k \in \mathbb{Z}$, and we conclude that $4 \mid a^2 - b^2$. ⊠

Question 2. Let $a \in \mathbb{Z}$. Show that $3 \mid a$ iff $3 \mid a^2$.

Proof. Assume $3 \mid a$. Then $a = 3n$ for some $n \in \mathbb{Z}$, so $a^2 = (3n)^2 = 9n^2 = 3(3n^2)$. Since $3n^2 \in \mathbb{Z}$, we have $3 \mid a^2$.

Conversely, assume that $3 \mid a^2$ and $3 \nmid a$ by contradiction. Then $a^2 = 3n$ for some $n \in \mathbb{Z}$, and either $a = 3k+1$ or $a = 3k+2$ for some $k \in \mathbb{Z}$.

Case 1: $a = 3k+1$ for some $k \in \mathbb{Z}$. Then $a^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Since $\mathbb{Z}$ is closed under multiplication and addition, we have $3k^2 + 2k \in \mathbb{Z}$. So a^2 is of the form $3m+1$ for some $m \in \mathbb{Z}$, which is a contradiction since $3 \mid a^2$.

Case 2: $a = 3k+2$ for some $k \in \mathbb{Z}$. It follows that $a^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 6k + 1) + 1$. Since $3k^2 + 6k + 1$ is an integer, a^2 is of the form $3m+1$ for some $m \in \mathbb{Z}$, a contradiction. We conclude that $3 \mid a$. ⊠

Question 3. Use the result from Question 2 to show that $\sqrt{3}$ is irrational.

Proof. We prove the desired result by contradiction. Assume $\sqrt{3}$ is rational, that is, it can be expressed in the form $\frac{m}{n}$ where $m, n \in \mathbb{Q}$, $n \neq 0$, and m and n are in lowest terms. Then $m = \sqrt{3}n$ which implies $m^2 = 3n^2$, which subsequently implies that $3 \mid m^2$. But then $3 \mid m$ by our previous result, and so $m = 3k$ for some $k \in \mathbb{Z}$. Therefore $3n^2 = (3k)^2 = 9k^2$, which implies that $n^2 = 3k^2$ which leads to the fact that $3 \mid n^2$. However, this implies $3 \mid n$ by our previous result, a contradiction since we assumed that m and n had no common divisors. Therefore $\sqrt{3}$ is irrational. ⊠

Question 4. Let $a, b \in \mathbb{R}$. Show that if $a + b$ is rational, then a is irrational or b is irrational.

Proof. Assume by the contrapositive statement that a is rational and b is irrational. We want to show that $a+b$ is not rational— we do this by contradiction.

Assume that $a + b \in \mathbb{Q}$, then $a + b = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$. We have $a = \frac{k}{q}$ by assumption. So

$$b = \frac{m}{n} - a = \frac{m}{n} - \frac{k}{q} = \frac{mq + nk}{nq}$$

which is rational since $\mathbb{Q}$ is a field. But b is irrational by assumption, a contradiction, and we are done. $\boxtimes$