Math 240: Introduction to Mathematical Thought

Homework 4, Solutions

Assigned exercises

4.2 Let $a, b \in \mathbb{Z}$, where $a \neq 0$, $b \neq 0$. Prove that if $a|b$ and $b|a$, then $a = b$ or $a = -b$.

Proof. We use a direct proof. Suppose that $a|b$ and $b|a$. Then $b = ac$ and $a = bd$ for some integers c, d. So

$$b = ac = (bd)c = bdc,$$

and since $b \neq 0$ we see that $dc = 1$. Since c and d are integers, by inspection the equation $dc = 1$ only has the solutions:

$$(c, d) = (1, 1) \text{ or } (c, d) = (-1, -1).$$

In the case where $(c, d) = (1, 1)$ we see that $a = b$; in the case where $(c, d) = (-1, -1)$ we see that $a = -b$.

□

4.4 Let $x, y \in \mathbb{Z}$. Prove that if $3 \not| x$ and $3 \not| y$, then $3|x^2 - y^2$.

Proof. We will use a direct proof and a case analysis. Assume that $3 \not| x$ and $3 \not| y$. Then we know that x and y are of the form $3k + 1$ or $3k + 2$ for some integer k. So we have four cases to consider. Let k and l denote integers.
Case 1: $x = 3k + 1$, $y = 3l + 1$
We have

$$\begin{aligned} x^2 - y^2 &= (3k + 1)^2 - (3l + 1)^2 \\ &= 9k^2 + 6k + 1 - (9l^2 + 6l + 1) \\ &= 3(3k^2 + 2k - 3l^2 - 2l); \end{aligned}$$

since $3k^2 + 2k - 3l^2 - 2l$ is an integer, we know that $3|x^2 - y^2$.
Case 2: $x = 3k + 1$, $y = 3l + 2$
We have

$$\begin{aligned} x^2 - y^2 &= (3k + 1)^2 - (3l + 2)^2 \\ &= 9k^2 + 6k + 1 - (9l^2 + 12l + 4) \\ &= 3(3k^2 + 2k - 3l^2 - 4l - 1); \end{aligned}$$

since $3k^2 + 2k - 3l^2 - 4l - 1$ is an integer, we know that $3|x^2 - y^2$.

Case 3: $x = 3k + 2$, $y = 3l + 1$
We have

$$\begin{aligned} x^2 - y^2 &= (3k+2)^2 - (3l+1)^2 \\ &= 9k^2 + 12k + 4 - (9l^2 + 6l + 1) \\ &= 3(3k^2 + 4k - 3l^2 - 2l + 1); \end{aligned}$$

since $3k^2+4k-3l^2-2l+1$ is an integer, we know that $3|x^2-y^2$.
Case 4: $x = 3k + 2$, $y = 3l + 2$
We have

$$\begin{aligned} x^2 - y^2 &= (3k+2)^2 - (3l+2)^2 \\ &= 9k^2 + 12k + 4 - (9l^2 + 12l + 4) \\ &= 3(3k^2 + 4k - 3l^2 - 4l); \end{aligned}$$

since $3k^2 + 4k - 3l^2 - 4l$ is an integer, we know that $3|x^2 - y^2$. □

4.18 Let $m, n \in \mathbb{N}$ such that $m \geq 2$ and $m|n$. Prove that if a and b are integers such that $a \equiv b \pmod{n}$, then $a \equiv b \pmod{m}$.

Proof. We use a direct proof. Let $m, n \in \mathbb{N}$ such that $m \geq 2$ and $m|n$. Suppose that $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{n}$. Then by definition

$$n|a - b.$$

Since $m|n$, we apply Result 4.1 (p. 100) (this is the statement that divisibility is transitive), to conclude that

$$m|a - b.$$

So by definition we know that $a \equiv b \pmod{m}$, as desired. □

Extra exercises

4.3 Let $m \in \mathbb{Z}$.

(a) *Proof.* Suppose that $3|m$. Then $m = 3k$ for some integer k. So

$$m^2 = (3k)^2 = 9k^2 = 3(3k^2).$$

Since $3k^2$ is an integer, we see that $3|m^2$, as desired. □

(b) If $3 \nmid m^2$, then $3 \nmid m$.

(c) *Proof.* Assume that $3 \not| m$. Then we consider two cases.
Case 1: $m = 3k + 1$ for some integer k
Then

$$m^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1.$$

This shows that $3 \not| m^2$.
Case 2: $m = 3k + 2$ for some integer k
Then

$$m^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1.$$

This shows that $3 \not| m^2$. □

(d) If $3|m^2$, then $3|m$.
(e) Let $m \in \mathbb{Z}$. Then $3|m$ if and only if $3|m^2$.

4.6 We did this one in class; see your class notes.

4.15 Let $a, b, c, n \in \mathbb{Z}$, where $n \geq 2$ (this isn't really necessary; the proof we are about to give works for any $n \in \mathbb{Z}$). Prove that if $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof. We use a direct proof. Suppose that $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$. Then we know that $a = b + nk$ and $a = c + nl$ for some integers k and l. Solving these two equations for b and c we have

$$b = a - nk, \quad c = a - nl.$$

Therefore

$$b - c = (a - nk) - (a - nl) = n(l - k);$$

since $l - k \in \mathbb{Z}$ we know that $n|b - c$. Hence, by definition, $b \equiv c \pmod{n}$. □

4.21 Let $a \in \mathbb{Z}$. Prove that $a^3 \equiv a \pmod{3}$.

Proof. We consider three cases.
Case 1: $a \equiv 0 \pmod{3}$
Then $a^3 \equiv 0^3 \equiv 0 \equiv a \pmod{3}$.
Case 2: $a \equiv 1 \pmod{3}$
Then $a^3 \equiv 1^3 \equiv 1 \equiv a \pmod{3}$.
Case 3: $a \equiv 2 \pmod{3}$
Then $a^3 \equiv 2^3 \equiv 8 \equiv 2 \equiv a \pmod{3}$.
In all cases we have $a^3 \equiv a \pmod{3}$. □