Mathematics 300

Quiz 24 **Name: Answer Key**

1. (a) Define $a \equiv b \pmod{n}$. (Include in your definition the conditions that a, b, and n must satisfy.)

Solution. Let a and b integers and n a positive integer. Then

$$a \equiv b \pmod{n}$$

means that $n \mid (a - b)$. $\square$

(b) Prove that if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Solution. Assume $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. This implies there are integers q_1 and q_2 such that

$$a - b = q_1 n \qquad \text{and} \qquad b - c = q_2 n.$$

Therefore

$$a - c = (a - b) + (b - c) = q_2 n + q_2 n = (q_1 + q_2)n = qn$$

where $q = q_1 + q_2 \in \mathbb{Z}$. Whence $n \mid (a - b)$ and therefore $a \equiv c \pmod{n}$. $\square$

(c) Show that for all integers a and b, that $(a+b)^2 \equiv a^2 + b^2 \pmod{2}$.

Solution.

$$\begin{aligned}(a+b)^2 &\equiv a^2 + 2ab + b^2 \pmod{2}\\ &\equiv a^2 + 0ab + b^2 \pmod{2} \qquad (\text{because } 2 \equiv 0 \pmod{2}).\\ &\equiv a^2 + b^2 \pmod{2}.\end{aligned}$$

$\square$

2. Show that $(a + b)^2 = a^2 + b^2$ if and only if $a = 0$ or $b = 0$.

Solution. We have to show two implications.
(A) $(a + b)^2 = a^2 + b^2$ implies $a = 0$ or $b = 0$, and
(B) $a = 0$ or $b = 0$ implies $(a + b)^2 = a^2 + b^2$.

Proof of (A). Assume that $(a + b)^2 = a^2 + b^2$. Now we do some algebra:

$$\begin{aligned}(a + b)^2 &= a^2 + b^2\\ a^2 + 2ab + b^2 &= a^2 + b^2\\ \not{a}^2 + 2ab + \not{b}^2 &= \not{a}^2 + \not{b}^2\\ 2ab &= 0\end{aligned}$$

This implies that $a = 0$ or $b = 0$.

Proof of (B). Assume that $a = 0$ or $b = 0$. Then we have two cases:

Case 1. $a = 0$. Then

$$(a + b)^2 = (0 + b)^2 = b^2 = 0^2 + b^2 = a^2 + b^2$$

as required.

Case 2. $b = 0$. Then

$$(a + b)^2 = (a + 0)^2 = a^2 = a^2 + 0^2 = a^2 + b^2.$$

And the required equation holds in this case also. □

3. Let abc be a three digit decimal number. (Thus for the number 347 we have $a = 3$, $b = 4$, and $c = 7$.) Use that $10 \equiv 1 \pmod 3$ to show

$$abc \equiv a + b + c \pmod 3.$$

Solution. This is an elementary calculation:

$$\begin{aligned} abc &= a(10)^2 + b(10) + c \\ &\equiv a(1)^2 + b(1) + c && \pmod 3 \\ &\equiv a + b + c && \pmod 3. \end{aligned}$$

□

4. (a) Let n be an integer. Show that if $3 \mid n^2$, then $3 \mid n$.

Solution. We prove the contrapositive: If $3 \nmid n$, then $3 \nmid n^2$. Assume that $3 \nmid n$. Then there are two cases:

Case 1. $n \equiv 1 \pmod 3$. Then

$$\begin{aligned} n^2 &\equiv 1^2 && \pmod 3 \\ &\equiv 1 && \pmod 3 \\ &\not\equiv 0 && \pmod 3 \end{aligned}$$

and therefore $3 \nmid n^2$ in this case.

Case 2. $n \equiv 2 \pmod 3$. Then

$$\begin{aligned} n^2 &\equiv 2^2 && \pmod 3 \\ &\equiv 4 && \pmod 3 \\ &\equiv 1 && \pmod 3 \\ &\not\equiv 0 && \pmod 3. \end{aligned}$$

Whence $3 \nmid n^2$ in this case. □

(b) Show that $\sqrt{3}$ is irrational.

Solution. Towards a contradiction assume that $\sqrt{3}$ is rational. Then we can express $\sqrt{3}$ as a fraction

$$\sqrt{3} = \frac{a}{b}$$

where a and b are integers, $b \neq 0$ and also we can assume that the fraction is in lowest terms. Now square both sides of $\sqrt{3} = a/b$ and multiply by b^2 to get

$$3b^2 = a^2.$$

This implies that $3 \mid a^2$ and so by Part (a) of this problem we have that $3 \mid a$. Therefore $a = 3a'$ for some integer a'. Use this in $3b^2 = a^2$:

$$3b^2 = (3a')^2 = 9(a')^2.$$

Divide by 3 to get

$$b^2 = 3(a')^2$$

which implies that $3 \mid b^2$. So we can again use Part (a) to conclude that $3 \mid b$ and thus $b = 3b'$ for some integer b'. Therefore we have

$$\frac{a}{b} = \frac{3a'}{3b'} = \frac{a'}{b'}.$$

This is a contradiction because the fraction $\frac{a}{b}$ was assumed to be in lowest terms. $\square$

5. Show that if r is rational, then so it $s = \dfrac{2r}{1+r^2}$.

Solution. Assume that r is a rational number. Then

$$r = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Use this in the formula for s.

$$\begin{aligned}
s &= \frac{2r}{1+r^2} \\
&= \frac{2\left(\frac{a}{b}\right)}{1+\left(\frac{a}{b}\right)^2} \\
&= \frac{\left(2\frac{a}{b}\right)b^2}{\left(1+\left(\frac{a}{b}\right)^2\right)b^2} && \text{(Multiply top and bottom by } b^2\text{)} \\
&= \frac{2ab}{a^2+b^2} \\
&= \frac{p}{q}
\end{aligned}$$

where $p = 2ab$ and $q = a^2 + b^2$ are integers. Also $q \neq 0$. Thus $s = p/q$ is a rational number. □

6. Use that $4 \cdot 5 \equiv 1 \pmod{19}$ to solve $5x \equiv 2 \pmod{19}$.

Solution. Multiply both sides of

$$5x \equiv 2 \pmod{19}$$

to get

$$20x \equiv 8 \pmod{19}$$

But $20 \equiv 1 \pmod{19}$ so this is equivalent to

$$x \equiv 8 \pmod{19}.$$

which is the solution. □

7. Let $A = \{5k : k \in \mathbb{Z}\}$ and $B = \{15a + 10b : a, b \in \mathbb{Z}\}$. Prove that $A = B$.

Solution. We need to prove two inclusions.

Proof of $B \subseteq A$. Let $x \in B$. Then for some integers a and b we have $x = 15a + 10b$. But this

$$x = 15a + 10b = 5(3a + 2b) = 5k$$

where $k = 3a + 2b$ is an integer. This shows that $x \in A$.

Proof of $A \subseteq B$ Let $x \in A$. Then $x = 5k$ for some $k \in \mathbb{Z}$. Therefore

$$x = 5k = (15 + (-10))k = 15k + 10(-k) = 15a + 10b$$

where $a = k$ and $b = -k$ are integers. Therefore $x \in A$.

Therefore we have proven $A \subseteq B$ and $B \subseteq A$, which shows that $A = B$. $\square$

8. State ***Bézout's Theorem***.

Solution. Let a and b be positive integers. Then there are integers x_0 and y_0 such that

$$ax_0 + by_0 = \gcd(a, b).$$

$\square$

9. (a) State the ***division algorithm***.

Solution. Let a and b be integers with $b > 0$. Then there are unique integers q and r such that

$$a = qb + r \qquad \text{and} \qquad 0 \le r < b.$$

$\square$

(b) Let $A = \{12x + 20y : x, y \in \mathbb{Z}\}$ and let d be the smallest positive element of A. Prove that $4 \mid d$.

Solution. As $d \in A$ there are integers x_0 and y_0 such that $d = 12x_0 + 20y_0$. Thus

$$d = 12x_0 + 20y_0 = 4(3x_0 + 5y_0) = 4n$$

where $n = 3x_0 + 5y_0$ is an integer. Thus $4 \mid d$. $\square$

(c) With notation as in (b) show that $d \mid 4$.

Solution. Again, as $d \in A$, there are integers x_0 and y_0 with

$$d = 12x_0 + 20y_0.$$

Towards a contradiction assume that $d \nmid 4$. Then by the division algorithm there are integers q and r such that

$$4 = qd + r \qquad \text{and} \qquad 0 < r < d.$$

(The reason $r > 0$ is that $4 \nmid d$.) Solve for r

$$\begin{aligned} r &= 4 - qd \\ &= 4 - q(12x_0 + 20y_0) && \text{(using } d = 12x_0 + 20y_0.\text{)} \\ &= (12(2) + 20(-1)) - q(12x_0 + 20y_0) && \text{(using } 4 = 12(2) + 20(-1)\text{)} \\ &= 12(2 - qx_0) + 20(-1 - qy_0) \\ &= 12x + 20y \end{aligned}$$

where $x = 2 - qx_0$ and $y = -1 - qy_0$ are integers. This shows that $r \in A$. But $0 < r < d$, therefore r is a positive element of A less than d, contradicting that d is the smallest positive element of A. $\square$