Mathematics 300 Homework, October 6, 2017.

You should read §5.3 (Pages 107–109) in the text. This is some guidelines for mathematical writing. Problems 3 and 4 on this sheet will be collected.

For the rest of this homework we will development a little of the theory of congruences. The official definition of $a \equiv b \pmod{n}$ is that $n \mid (a-b)$. This means that this is an integer q such that $a - b = qn$. We will often just jump from the statement that "$a \equiv b \pmod{n}$" to saying that "there is an integer q such that $a - b = qn$ without writing the intermediate step that of saying that $n \mid (a-b)$.

Proposition 1. *For all $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ the congruence $a \equiv a \pmod{n}$ holds.*

Proof. We have $a - a = 0$ and $n \mid 0$, so $a \equiv a \pmod{n}$ by the definition of congruence. $\square$

Proposition 2. *If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*

Proof. We are given $a \equiv b \pmod{n}$. Therefore there is an integer q such that

$$a - b = qn.$$

Therefore

$$b - a = -(a - b) = (-q)n$$

and $-q$ is an integer. Thus $n \mid (b - a)$ which shows that $b \equiv a \pmod{n}$. $\square$

Proposition 3. *If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proof. We are given $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Therefore there are integers q_1 and q_2 such that

$$\begin{aligned} a - b &= q_1 n \\ b - c &= q_2 n \end{aligned}$$

Therefore (and here we use that add and subtract the same quantity trick):

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

and $q_1 + q_2 \in \mathbb{Z}$ which shows that $n \mid (a - c)$ and so $a \equiv c \pmod{n}$. $\square$

Proposition 4. *If $a \equiv b \pmod{n}$ and $c \equiv d$ then $a + c \equiv b + d \pmod{n}$.*

Proof. We are given $a \equiv b \pmod{n}$ and $c \equiv d$ and therefore there are integers q_1 and q_2 such that

$$\begin{aligned} a - b &= q_1 n \\ c - d &= q_2 n. \end{aligned}$$

Therefore

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

and $q_1 + q_2 \in \mathbb{Z}$. Therefore $n \mid \big((a + c) - (b - d)\big)$. This shows that $a + c \equiv b + d \pmod{n}$ as required. $\square$

Proposition 5. *If* $a \equiv b \pmod{n}$ *then for any* $c \in \mathbb{Z}$ *the congruence* $ac \equiv bc \pmod{n}$ *holds.*

Problem 1. Prove this. (For solution page down.) $\square$

Proposition 6. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$*, then* $ac \equiv bd \pmod{n}$*.*

Problem 2. Prove this. *Hint:* One way to combine Proposition 5 with Proposition 3.

Problem 3. Show that if two integers, x and y, have the same parity, then $x \equiv y \pmod{2}$.

Problem 4. Let n be a positive integer. Show that if $a, b \in \mathbb{Z}$ have the same remainder when divided by n, then $a \equiv b \pmod{n}$.

Proof of Proposition 5. We are given $a \equiv b \pmod{n}$. Therefore there is an integer q such that

$$a - b = qn.$$

Then

$$ac - bc = (a - b)c = qnc$$

and qn is an integer. Thus $n \mid (ac - bc)$, which implies $ac \equiv bc \pmod{n}$. □

First proof of Proposition 6. We are given the two congruences

$$\begin{aligned} a &\equiv b \pmod{n} \\ c &\equiv d \pmod{n} \end{aligned}$$

By Proposition 5 we can multiply the first of these by c get

$$ac \equiv bc \pmod{n}.$$

We can then use Proposition 5 again to multiply both sides of $c \equiv d \pmod{n}$ by b to get

$$bc \equiv bd \pmod{n}.$$

We can now use the transitive property of Proposition 3 to conclude that

$$\begin{aligned} ac &\equiv bc \pmod{n} \\ &\equiv bd \pmod{n} \end{aligned}$$

and thus $ac \equiv bd$. □

Second proof of Proposition 6. We are given the two congruences

$$\begin{aligned} a &\equiv b \pmod{n} \\ c &\equiv d \pmod{n}. \end{aligned}$$

These imply that there are integers q_1 and q_2 such that

$$\begin{aligned} a - b &= q_1 n \\ c - d &= q_2 n \end{aligned}$$

Then (and this is a more sophisticated version of the add and subtract the same quantity trick)

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a - b)c + b(c - d) \\ &= (q_1 n)c + b(q_2 n) \\ &= (q_1 c + q_2 b)n \end{aligned}$$

and $q_1 c + q_2 b$ is an integer. Thus $n \mid (ac - bd)$ which shows that $ac \equiv bd \pmod{n}$. □