Problems to Week 12 Tutorial — MACM 101 (Spring 2025)

Problem 1. Determine whether each of the following pairs of integers are congruent modulo 9.

$$(i)\ 76, 243 \qquad (ii)\ -137, 700 \qquad (iii)\ -56, -1199$$

Answer.

Two integers are congruent modulo 9 precisely when they have the same remainder modulo 9. So we divide each by 9 and record the remainder.

	first integer	second integer	congruent?
(i)	$76 \equiv 4$	$243 \equiv 0$	No
(ii)	$-137 \equiv 7$	$700 \equiv 7$	Yes
(iii)	$-56 \equiv 7$	$-1199 \equiv 7$	Yes

$(\mathrm{mod} 9)$.

Problem 2. For each of the following, determine the values of the integers $n > 1$ for which the given congruence is true:

$$(a)\ 28 \equiv 6 \pmod{n} \qquad (b)\ 68 \equiv 37 \pmod{n}.$$

Answer.

(a) We have $28 \equiv 6 \pmod{n}$ if and only if $n \mid (28-6) = 22$. Since $n > 1$, the possible values are

$$n = 2, 11, 22.$$

(b) We have $68 \equiv 37 \pmod{n}$ if and only if $n \mid (68 - 37) = 31$. Since 31 is prime, the only possible value is

$$n = 31.$$

Problem 3. Let $n \in \mathbb{Z}$. Prove that $n(n+1)(n+2)$ is divisible by 3.

Answer.

The integers $n, n+1, n+2$ are three consecutive integers, so exactly one of them is congruent to 0 modulo 3. Therefore one of the three factors is divisible by 3, and hence

$$3 \mid n(n+1)(n+2).$$

Problem 4. Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ and let $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ if and only if $a \equiv b \pmod{mn}$.

Answer.

Suppose first that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. Then

$$m \mid (a-b) \quad \text{and} \quad n \mid (a-b).$$

Since $\gcd(m, n) = 1$, it follows that $mn \mid (a-b)$. Thus $a \equiv b \pmod{mn}$.
Conversely, if $a \equiv b \pmod{mn}$, then $mn \mid (a-b)$. Since both m and n divide mn, we obtain $m \mid (a-b)$ and $n \mid (a-b)$. Therefore $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

Problem 5. If $n \in \mathbb{N}$ and $n > 2$, prove that

$$\sum_{i=1}^{n-1} i \equiv \begin{cases} 0, & n \text{ odd}, \\ \dfrac{n}{2}, & n \text{ even} \end{cases} \pmod{n}.$$

Answer.

Using the formula for the sum of the first $n-1$ positive integers,

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}.$$

If n is odd, then $(n-1)/2$ is an integer, so this sum is a multiple of n and is therefore congruent to 0 modulo n.
If n is even, then

$$\frac{n(n-1)}{2} - \frac{n}{2} = \frac{n(n-2)}{2} = n\left(\frac{n-2}{2}\right),$$

which is a multiple of n. Hence the sum is congruent to $n/2$ modulo n.

Problem 6. How many proper divisors of 0 are there in $\mathbb{Z}_{17}$ and in $\mathbb{Z}_{25}$?

Answer.

In $\mathbb{Z}_{17}$, every nonzero element is invertible because 17 is prime. Thus there are no proper divisors of 0.
In $\mathbb{Z}_{25}$, a nonzero element is a divisor of 0 precisely when it is not relatively prime to 25. These elements are

$$\overline{5},\ \overline{10},\ \overline{15},\ \overline{20}.$$

Therefore the numbers of proper divisors of 0 are, respectively,

$$0 \text{ in } \mathbb{Z}_{17} \quad \text{and} \quad 4 \text{ in } \mathbb{Z}_{25}.$$

Problem 7. Find the inverse of $5 \pmod{13}$. Find the inverse of $22 \pmod{27}$.

Answer.

Since

$$5 \cdot 8 = 40 \equiv 1 \pmod{13},$$

the inverse of 5 modulo 13 is 8.
Also,

$$22 \cdot 16 = 352 = 13 \cdot 27 + 1,$$

so $22 \cdot 16 \equiv 1 \pmod{27}$. Thus the inverse of 22 modulo 27 is 16.

Problem 8. Solve the following system of linear congruences:

$$\begin{aligned} x &\equiv 2 \pmod{11}, \\ x &\equiv 1 \pmod{7}. \end{aligned}$$

Answer.

Write $x = 2 + 11k$. Substituting into the second congruence gives

$$2 + 11k \equiv 1 \pmod{7},$$

and hence $4k \equiv 6 \pmod{7}$. The inverse of 4 modulo 7 is 2, so

$$k \equiv 12 \equiv 5 \pmod{7}.$$

Thus $k = 5 + 7t$ for some $t \in \mathbb{Z}$, and therefore

$$x = 2 + 11(5 + 7t) = 57 + 77t.$$

Equivalently, the solution is

$$x \equiv 57 \pmod{77}.$$

Problem 9. For $a, b, n \in \mathbb{Z}$ and $n > 1$, prove that

$$a \equiv b \pmod{n} \quad \Longrightarrow \quad \gcd(a, n) = \gcd(b, n).$$

Answer.

Since $a \equiv b \pmod{n}$, there is an integer k such that $a - b = kn$. If an integer d divides both a and n, then

$$d \mid a - kn = b,$$

so d also divides both b and n. The same argument, with a and b interchanged, shows that every common divisor of b and n is also a common divisor of a and n. The two pairs therefore have the same common divisors, and hence

$$\gcd(a, n) = \gcd(b, n).$$