math 228

Sample Midterm Examination Solutions

Question 1. Find **all** solutions $x \in \mathbb{Z}_{126}$ of the equation $11 \cdot x = 12$.

SOLUTION: We use the Euclidean algorithm to find the greatest common divisor $d = (11, 126)$:

$$\begin{aligned} 126 &= 11 \cdot 11 + 5 \\ 11 &= 2 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

and the last nonzero remainder is $d = (11, 126) = 1$. Therefore the equation $11 \cdot x = 12$ has exactly $d = 1$ solution in $\mathbb{Z}_{126}$.

In order to find the solution, we work backward, writing $d = 1$ as a linear combination of 11 and 126,

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2 \cdot (126 - 11 \cdot 11) \\ &= 23 \cdot 11 - 2 \cdot 126, \end{aligned}$$

so that $1 = 23 \cdot 11 + (-2) \cdot 126$. Multiplying this equation by 12, we have

$$11 \cdot (12 \cdot 23) = 12 + 2 \cdot 12 \cdot 126,$$

and the unique solution is $x = [\,12 \cdot 23\,] = [\,24\,]$ in $\mathbb{Z}_{126}$.

Question 2.

(a) Show that if $n \in \mathbb{N}$, then $10^n \equiv (-1)^n \pmod{11}$.
Hint: Use induction!

(b) Let $m = a_k a_{k-1} \cdots a_1 a_0$ be the decimal expansion of the nonnegative integer m. Show that $11 \mid m$ if and only if $11 \mid \sum_{i=0}^{k} (-1)^i a_i$.

SOLUTION:

(a) We use induction to show that

$$10^n \equiv (-1)^n \pmod{11} \qquad (*)$$

for all nonnegative integers n.

Base Case: For $n = 0$, we have $10^0 = 1 = (-1)^0$, and $(*)$ is true for $n = 1$.

Inductive Step: Assume that $(*)$ is true for some $n \geq 0$, then

$$10^{n+1} \equiv 10 \cdot 10^n \equiv (-1) \cdot (-1)^n \equiv (-1)^{n+1} \pmod{11},$$

so that $(*)$ is true for $n + 1$ also.

By the Principle of Mathematical Induction, $(*)$ is true for all $n \geq 0$.

(b) If $m \geq 0$, then m has a unique decimal expansion given by

$$m = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k$$

where $0 \leq a_i \leq 9$ for $i = 0, 1, \ldots, k$. Therefore, from part (a),

$$m \equiv a_0 \cdot (-1)^0 + a_1 \cdot (-1)^1 + a_2 \cdot (-1)^2 + \cdots + a_k \cdot (-1)^k \pmod{11},$$

so that $m \equiv 0 \pmod{11}$ if and only if $\sum_{i=0}^{k} (-1)^i a_i \equiv 0 \pmod{11}$, that is, $11 \mid m$ if and only if $11 \mid \sum_{i=0}^{k} (-1)^i a_i$.

Question 3.

(a) Let ℓ, m, and n be integers, with $\ell > 0$. Show that $(\ell m, \ell n) = \ell(m, n)$.

(b) Let m and n be nonzero integers. Assuming that $d = (m, n)$, show that $\frac{m}{d}$ and $\frac{n}{d}$ are relatively prime.

SOLUTION: .

(a) Let $d = (m, n)$, from the Euclidean algorithm there exist integers u and v such that

$$d = mu + nv,$$

so that the positive integer

$$\ell d = \ell mu + \ell nv$$

is a linear combination of ℓm and ℓn, and therefore

$$(\ell m, \ell n) \leq \ell mu + \ell nv = \ell d.$$

On the other hand, ℓd is a common divisor of ℓm and ℓn, so that

$$\ell d \leq (\ell m, \ell n).$$

Therefore $(\ell m, \ell n) = \ell(m, n)$.

(b) Let $d = (m, n)$, then from part (a) we have

$$d = (m, n) = \left(d\frac{m}{d}, d\frac{n}{d}\right) = d\left(\frac{m}{d}, \frac{n}{d}\right),$$

and since $d \geq 1$, from the cancellation law we have $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Question 4. Given positive integers m and n, consider the set

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,\, b,\, c,\, d \in \mathbb{Z},\ m \mid b,\ \text{and } n \mid c \right\}.$$

Show that ordinary matrix addition and multiplication make S a ring with identity. Is S commutative?

Hint: Show that S is a subring of $M_2(\mathbb{Z})$, the ring of all 2×2 matrices with entries in $\mathbb{Z}$.

SOLUTION: Since S is a subset of the ring $M_2(\mathbb{Z})$ and $O_{M_2(\mathbb{Z})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$, we only have to show it is closed under addition and multiplication and that it contains additive inverses.

Note that if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ are in S, then $m \mid b,\ m \mid f$ and $n \mid c,\ n \mid g$.

Now,

$$A + B = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

and $m \mid b+f$, and $n \mid c+g$, so that $A + B \in S$.

Also,

$$A \cdot B = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

and $m \mid af+bh$, and $n \mid +dg$ so that $A \cdot B \in S$.

Finally,

$$-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

and $m \mid -b$, and $n \mid -c$, so that $-A \in S$.

Therefore S is a subring of $M_2(\mathbb{Z})$, and since $m \mid 0$ and $n \mid 0$, then $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$, and S is a ring with identity.

Note that S is noncommutative since

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} = \begin{pmatrix} 1+mn & m \\ n & 1 \end{pmatrix},$$

while

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m \\ n & 1+mn \end{pmatrix},$$

and these are not the same since $mn > 0$.

Question 5. Let m and n be positive integers. Assuming that $(m,n)=1$ and the integer $m\cdot n$ is a perfect square, that is, $m\cdot n=k^2$ for some positive integer k, show that both m and n are squares.

Hint: Prime Factorization!

SOLUTION: Suppose that m and n are positive integers and $m\cdot n=k^2$ for some positive integer $k>1$, and suppose the prime factorization of k is given by

$$k=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}\cdot q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$$

where $p_1<p_2<\cdots<p_r$ are distinct primes that k has in common with m, and $q_1<q_2<\cdots<q_s$ are distinct primes that k has in common with n, and $\alpha_i\geq 1,\ \beta_j\geq 1$ for $1\leq i\leq r$ and $1\leq j\leq s$.

Since $(m,n)=1$, then no p_i is equal to a q_j, and therefore

$$m\cdot n=k^2=p_1^{2\alpha_1}p_2^{2\alpha_2}\cdots p_r^{2\alpha_r}\cdot q_1^{2\beta_1}q_2^{2\beta_2}\cdots q_s^{2\beta_s},$$

implies that

$$m=p_1^{2\alpha_1}p_2^{2\alpha_2}\cdots p_r^{2\alpha_r}\qquad\text{and}\qquad n=q_1^{2\beta_1}q_2^{2\beta_2}\cdots q_s^{2\beta_s},$$

so that m and n are both perfect squares.

Question 6. The three children in a family have feet that are 7 inches, 9 inches, and 11 inches in length. When they measure the length of the living room of their house using their feet, they find that there are 2, 3, and 4 inches left over, respectively. How long is the living room?

Hint: Chinese Remainder Theorem!

SOLUTION: Let $x=$ the length of the living room (measured in inches), then we want to solve the system of linear congruences

$$\begin{aligned} x &\equiv 2 \pmod 7\\ x &\equiv 3 \pmod 9\\ x &\equiv 4 \pmod{11}\end{aligned}$$

We have $a_1=2$, $a_2=3$, and $a_3=4$, while $m_1=7$, $m_2=9$, and $m_3=11$. Letting $M=7\cdot 9\cdot 11$, then

$$M_1=9\cdot 11=99,\qquad M_2=7\cdot 11=77,\qquad M_3=7\cdot 9=63$$

and we solve the congruences:

$$\begin{aligned} M_1y_1 &\equiv 1 \pmod 7 \quad &&\text{implies} \quad && y_1 \equiv 1 \pmod 7\\ M_2y_2 &\equiv 1 \pmod 9 \quad &&\text{implies} \quad && y_2 \equiv 2 \pmod 9\\ M_3y_3 &\equiv 1 \pmod{11} \quad &&\text{implies} \quad && y_3 \equiv 7 \pmod{11}\end{aligned}$$

The solution is

$$x\equiv a_1M_1y_1+a_2M_2y_2+a_3M_3y_3\equiv 2\cdot 99\cdot 1+3\cdot 77\cdot 2+4\cdot 63\cdot 7\equiv 2424 \pmod{693},$$

that is, $x=345$ inches, or $x=28.75$ feet.