Question 1. [Exercises 2.1, # 12]

Which of the following congruences have solutions:
(a) \( x^2 \equiv 1 \pmod{3} \) (b) \( x^2 \equiv 2 \pmod{7} \) (c) \( x^2 \equiv 3 \pmod{11} \)

Solution:

(a) Note that
\[
\begin{align*}
x &\equiv 0 \pmod{3} \quad \text{implies} \quad x^2 \equiv 0 \pmod{3} \\
x &\equiv 1 \pmod{3} \quad \text{implies} \quad x^2 \equiv 1 \pmod{3} \\
x &\equiv 2 \pmod{3} \quad \text{implies} \quad x^2 \equiv 1 \pmod{3}
\end{align*}
\]

and the congruence \( x^2 \equiv 1 \pmod{3} \) has a solution if and only if \( x \equiv 1 \pmod{3} \) or \( x \equiv 2 \pmod{3} \).

(b) Note that
\[
\begin{align*}
x &\equiv 0 \pmod{7} \quad \text{implies} \quad x^2 \equiv 0 \pmod{7} \\
x &\equiv 1 \pmod{7} \quad \text{implies} \quad x^2 \equiv 1 \pmod{7} \\
x &\equiv 2 \pmod{7} \quad \text{implies} \quad x^2 \equiv 4 \pmod{7} \\
x &\equiv 3 \pmod{7} \quad \text{implies} \quad x^2 \equiv 2 \pmod{7} \\
x &\equiv 4 \pmod{7} \quad \text{implies} \quad x^2 \equiv 2 \pmod{7} \\
x &\equiv 5 \pmod{7} \quad \text{implies} \quad x^2 \equiv 4 \pmod{7} \\
x &\equiv 6 \pmod{7} \quad \text{implies} \quad x^2 \equiv 1 \pmod{7}
\end{align*}
\]

and the congruence \( x^2 \equiv 2 \pmod{7} \) has a solution if and only if \( x \equiv 3 \pmod{7} \) or \( x \equiv 4 \pmod{7} \).

(c) Note that
\[
\begin{align*}
x &\equiv 0 \pmod{11} \quad \text{implies} \quad x^2 \equiv 0 \pmod{11} \\
x &\equiv 1 \pmod{11} \quad \text{implies} \quad x^2 \equiv 1 \pmod{11} \\
x &\equiv 2 \pmod{11} \quad \text{implies} \quad x^2 \equiv 4 \pmod{11} \\
x &\equiv 3 \pmod{11} \quad \text{implies} \quad x^2 \equiv 9 \pmod{11} \\
x &\equiv 4 \pmod{11} \quad \text{implies} \quad x^2 \equiv 5 \pmod{11} \\
x &\equiv 5 \pmod{11} \quad \text{implies} \quad x^2 \equiv 3 \pmod{11} \\
x &\equiv 6 \pmod{11} \quad \text{implies} \quad x^2 \equiv 3 \pmod{11} \\
x &\equiv 7 \pmod{11} \quad \text{implies} \quad x^2 \equiv 5 \pmod{11} \\
x &\equiv 8 \pmod{11} \quad \text{implies} \quad x^2 \equiv 9 \pmod{11} \\
x &\equiv 9 \pmod{11} \quad \text{implies} \quad x^2 \equiv 4 \pmod{11} \\
x &\equiv 10 \pmod{11} \quad \text{implies} \quad x^2 \equiv 1 \pmod{11}
\end{align*}
\]

and the congruence \( x^2 \equiv 3 \pmod{11} \) has a solution if and only if \( x \equiv 5 \pmod{11} \) or \( x \equiv 6 \pmod{11} \).
Question 2. [Exercises 2.1, # 32]

Let \( a, b, n \) be integers with \( n > 0 \). If \( (a, n) \) does not divide \( b \), prove that the congruence \( ax \equiv b \pmod{n} \) has no solution.

SOLUTION: Suppose that \( x_0 \) is a solution to the congruence \( ax \equiv b \pmod{n} \), then \( ax = b + kn \) for some integer \( k \), so that if \( d = (a, n) \), then \( d \mid b \).

The (equivalent) contrapositive statement says that if \( d = (a, n) \) does not divide \( b \), then the congruence \( ax \equiv b \pmod{n} \) has no solution.

Question 3. [Exercises 2.2, # 8].

(a) Solve the equation \( x^2 + x = 0 \) in \( \mathbb{Z}_5 \).

(b) Solve the equation \( x^2 + x = 0 \) in \( \mathbb{Z}_6 \).

(c) If \( p \) is prime, prove that the only solutions of \( x^2 + x = 0 \) in \( \mathbb{Z}_p \) are \( 0 \) and \( p - 1 \).

Solution:

(a) In \( \mathbb{Z}_5 \),

\[
\begin{align*}
0^2 + 0 &= 0 \\
1^2 + 1 &= 2 \\
2^2 + 2 &= 1 \\
3^2 + 3 &= 2 \\
4^2 + 4 &= 0
\end{align*}
\]

and the solutions to \( x^2 + x = 0 \) in \( \mathbb{Z}_5 \) are \( x = 0, 4 \).

(b) In \( \mathbb{Z}_6 \),

\[
\begin{align*}
0^2 + 0 &= 0 \\
1^2 + 1 &= 2 \\
2^2 + 2 &= 0 \\
3^2 + 3 &= 0 \\
4^2 + 4 &= 2 \\
5^2 + 5 &= 0
\end{align*}
\]

and the solutions to \( x^2 + x = 0 \) in \( \mathbb{Z}_6 \) are \( x = 0, 2, 3, 5 \).

(c) If \( p \) is a prime, then \( a^2 + a \equiv 0 \pmod{p} \) if and only if \( p \mid a(a+1) \), that is, if and only if \( p \mid a \) or \( p \mid a + 1 \), that is, if and only if \( a \equiv 0 \pmod{p} \) or \( a \equiv -1 \equiv p - 1 \pmod{p} \).

Therefore, If \( p \) is a prime, and \( x = [a] \in \mathbb{Z}_p \), then \( x^2 + x = 0 \) if and only if \( a^2 + a \equiv 0 \pmod{p} \), that is, if and only if \( a \equiv 0 \pmod{p} \) or \( a \equiv p - 1 \pmod{p} \), that is, if and only if \( x = 0 \) or \( x = p - 1 \) in \( \mathbb{Z}_p \).
Question 4. [Exercises 2.2, # 10].

(a) Find all $a$ in $\mathbb{Z}_5$ for which the equation $ax = 1$ has a solution. Then do the same thing for
(b) $\mathbb{Z}_4$  (c) $\mathbb{Z}_3$  (d) $\mathbb{Z}_6$

Solution: From Question 7 we note that if $n > 1$, then the equation $[a]x = [1]$ has a solution in $\mathbb{Z}_n$ if and only if $(a, n) = 1$.

(a) For $n = 5$, the equation $[a]x = 1$ has a solution in $\mathbb{Z}_5$ if and only if $(a, 5) = 1$, that is, if and only if $a = 1, 2, 3, 4$, and therefore the equation $ax = 1$ has a solution in $\mathbb{Z}_5$ if and only if $a = [1], [2], [3], [4]$.

(b) For $n = 4$, the equation $[a]x = 1$ has a solution in $\mathbb{Z}_4$ if and only if $(a, 4) = 1$, that is, if and only if $a = 1, 3$, and therefore the equation $ax = 1$ has a solution in $\mathbb{Z}_4$ if and only if $a = [1], [3]$.

(c) For $n = 3$, the equation $[a]x = 1$ has a solution in $\mathbb{Z}_3$ if and only if $(a, 3) = 1$, that is, if and only if $a = 1, 2$, and therefore the equation $ax = 1$ has a solution in $\mathbb{Z}_3$ if and only if $a = [1], [2]$.

(d) For $n = 6$, the equation $[a]x = 1$ has a solution in $\mathbb{Z}_6$ if and only if $(a, 6) = 1$, that is, if and only if $a = 1, 5$, and therefore the equation $ax = 1$ has a solution in $\mathbb{Z}_6$ if and only if $a = [1], [5]$.

Question 5. [Exercises 2.3, # 2].

How many solutions does the equation $6x = 4$ have in

(a) $\mathbb{Z}_7$?  (b) $\mathbb{Z}_8$?  (c) $\mathbb{Z}_9$?  (d) $\mathbb{Z}_{10}$?

Solution: Recall that the equation $[a]x = [b]$ has a solution in $\mathbb{Z}_n$ if and only if $(a, n) | b$, and in this case there are exactly $d = (a, n)$ distinct (modulo $n$) solutions.

(a) If $n = 7$, then $d = (6, 7) = 1$ and $1 | 4$, so that the equation $6x = 4$ has $d = 1$ solution in $\mathbb{Z}_7$.

(b) If $n = 8$, then $d = (6, 8) = 2$ and $2 | 4$, so that the equation $6x = 4$ has $d = 2$ solutions in $\mathbb{Z}_8$.

(c) If $n = 9$, then $d = (6, 9) = 3$ and $3 | 4$, so that the equation $6x = 4$ has no solutions in $\mathbb{Z}_9$.

(d) If $n = 10$, then $d = (6, 10) = 2$ and $2 | 4$, so that the equation $6x = 4$ has $d = 2$ solutions in $\mathbb{Z}_{10}$.

Question 6. [Exercises 2.3, # 4].

If $n$ is composite, prove that there exist $a, b \in \mathbb{Z}_n$ such that $a \neq 0$ and $b \neq 0$ but $ab = 0$.

Solution: If $n$ is composite then there exist integers $a$ and $b$ with $0 < a < n$ and $0 < b < n$ such that $ab = n$. Therefore $ab = 0$ in $\mathbb{Z}_n$, but since $n \nmid a$ and $n \nmid b$, then $a \neq 0$ and $b \neq 0$ in $\mathbb{Z}_n$.

Question 7. [Exercises 2.3, # 6].

Let $a$ and $n$ be integers with $n > 1$. Prove that $(a, n) = 1$ in $\mathbb{Z}$ if and only if the equation $[a]x = [1]$ in $\mathbb{Z}_n$ has a solution.

Solution: Suppose that $(a, n) = 1$, then there exist integers $u$ and $v$ such that $1 = au + nv$, so that $au \equiv 1$ (mod n). Letting $x = [u]$ then $x$ is a solution to the equation $[a]x = [1]$ in $\mathbb{Z}_n$.

Conversely, suppose that $[x_0]$ is a solution to the equation $[a]x = [1]$ in $\mathbb{Z}_n$, then $ax_0 \equiv 1$ (mod n) so that $ax_0 = 1 + kn$ for some integer $k$. However this means that 1 is a linear combination (with integer coefficients) of $a$ and $n$, and is the smallest such positive integer, therefore $(a, n) = 1$.
Question 8. [Exercises 2.3, # 12].

Let $a, b, n$ be integers with $n > 1$. Describe the solutions in $\mathbb{Z}$ of the congruence $ax \equiv b \pmod{n}$.

SOLUTION: Let $d = (a, n)$, we know that the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d \mid b$, and in this case it has exactly $d$ solutions which are distinct modulo $n$.

In the case that $d \mid b$, we find the solutions as in class. Since $d \mid a$ and $d \mid b$, then we can write

$$a = a_1d, \quad b = b_1d, \quad \text{and} \quad n = n_1d$$

for some integers $a_1, b_1$, and $n_1$. Also, from the Euclidean algorithm there exist integers $u$ and $v$ such that

$$d = au + nv,$$

so that $a_1u + n_1v = 1$. Multiplying this equation by $b$ we have

$$a_1ub + n_1vb = b,$$

that is, since $a_1ub = a_1u db_1 = a_1dub_1 = aub_1$, we have

$$aub_1 + nvb_1 = b.$$

Therefore, the integer $x_0 = ub_1$ is a solution to the congruence $ax \equiv b \pmod{n}$, and the $d$ incongruent solutions (modulo $n$) are given by

$$x_k = ub_1 + kn_1$$

for $0 \leq k \leq d - 1$. 