Comments on Congruences:

• When solving congruences, write \((\text{mod } m)\) for each simplified form of the congruence.

• Solving a congruence means finding the set of all integer solutions. Check your solution by substituting the smallest integer in your solution set for \(x\) in the original congruence.

• Don’t write your solution as \(x = \{3 + 11k \mid k \in \mathbb{Z}\}\). How can the variable \(x\), which is not a set, be equal to a set?

• On Learning Celebration #4, I will ask you to use the Euclidean algorithm and back substitution to solve a congruence. Many of the congruences in Exercise 4.4.8 are easy to solve by using tricks (or guess-and-check), and that’s fine for this homework assignment, but trickery and guess-and-check will not be fine on the learning celebration!

Comments on Induction:

• Induction is essential! If you’re struggling, come see me!

• State the claims! The range of possible values of \(n\) is crucial for induction and must be included in the claim!

• Be very explicit about what is being assumed (the claim for \(n = k\)), and don’t state the claim for \(n = k + 1\) as if you are assuming it is true! Write what the claim looks like for \(n = k + 1\) on your scratch paper as a guide for what you have to prove in the inductive step. If you ever write down what you are trying to prove within your proof, then you must make it very clear that you are trying to prove it, rather than stating it to be true.

• The computation in the inductive step is often much easier if you use factoring, rather than expanding out the polynomials.

• The word “namely” indicates that you are merely rephrasing a statement. For instance, we write “Now assume the claim is true for some \(n = k \in \mathbb{Z}_{\geq 1}\), namely ...” because we are just going to rephrase what it means for the claim to be true for \(n = k\). This is clearer than using a word like “so”, “thus”, or “then” that indicates that one statement implies another statement.
Exercise 4.4.8

(a) Solve $10x + 3 \equiv 0 \pmod{11}$.

*Solution:* We run the Euclidean algorithm on 11 and 10:

\[
\begin{align*}
11 &= 1 \cdot 10 + 1 \\
10 &= 10 \cdot 1 + 0,
\end{align*}
\]

so $\gcd(10, 11) = 1$, so the congruence has solutions. Back substitution yields $1 = 11 - 1 \cdot 10$, so the multiplicative inverse of 10 modulo 11 is $-1$, namely $-1 \cdot 10 \equiv 1 \pmod{11}$. Thus we can solve for $x$:

\[
\begin{align*}
10x + 3 &\equiv 0 \pmod{11}; \\
10x &\equiv 8 \pmod{11}; \\
x &\equiv -1 \cdot 8 \equiv 3 \pmod{11}.
\end{align*}
\]

So the set of integer solutions is $\{3 + 11k \mid k \in \mathbb{Z}\}$.

(b) Solve $9x \equiv 0 \pmod{11}$.

*Solution:* We run the Euclidean algorithm on 11 and 9:

\[
\begin{align*}
11 &= 1 \cdot 9 + 2 \\
9 &= 9 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0,
\end{align*}
\]

so $\gcd(9, 11) = 1$, so the congruence has solutions. Back substitution yields

\[
1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 1 \cdot 9) = 5 \cdot 9 - 4 \cdot 11,
\]

so $5 \cdot 9 \equiv 1 \pmod{11}$. Thus we can solve for $x$:

\[
\begin{align*}
9x &\equiv 0 \pmod{11}; \\
x &\equiv 5 \cdot 0 \equiv 0 \pmod{11}.
\end{align*}
\]

So the set of integer solutions is $\{11k \mid k \in \mathbb{Z}\}$.

(c) Solve $21x + 40 \equiv 0 \pmod{44}$.

*Solution:* We run the Euclidean algorithm on 44 and 21:

\[
\begin{align*}
44 &= 2 \cdot 21 + 2 \\
21 &= 10 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0.
\end{align*}
\]
Thus $\gcd(21, 44) = 1$, so the congruence has solutions. Back substitution yields

$$1 = 21 - 10 \cdot 2 = 21 - 10 \cdot (44 - 2 \cdot 21) = 21 \cdot 21 - 10 \cdot 44,$$

so $21 \cdot 21 \equiv 1 \pmod{44}$. Thus we can solve for $x$:

$$21x + 40 \equiv 0 \pmod{44};$$
$$21x \equiv 4 \pmod{44};$$
$$x \equiv 21 \cdot 4 = 84 \equiv 40 \pmod{44}.$$

So the set of integer solutions is $\{40 + 44k \mid k \in \mathbb{Z}\}$.

(d) Solve $33x + 1 \equiv 0 \pmod{44}$.

**Solution:** We run the Euclidean algorithm on $44$ and $33$:

$$44 = 1 \cdot 33 + 11$$
$$33 = 3 \cdot 11 + 0,$$

so $\gcd(33, 44) = 11$. Since $11 \nmid 1$, the congruence has no solutions.

(e) Solve $36x + 24 \equiv 0 \pmod{48}$.

We run the Euclidean algorithm on $48$ and $36$:

$$48 = 1 \cdot 36 + 12$$
$$36 = 3 \cdot 12 + 0,$$

so $\gcd(36, 48) = 12$. Since $12 \mid 24$, the original congruence has the same solutions as the congruence

$$3x + 2 \equiv 0 \pmod{4}.$$

We run the Euclidean algorithm on $4$ and $3$:

$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

and back substitution yields $1 = 4 - 1 \cdot 3$. Thus $-1 \cdot 3 \equiv 1 \pmod{4}$, so we can solve for $x$:

$$3x + 2 \equiv 0 \pmod{4};$$
$$3x \equiv 2 \pmod{4};$$
$$x \equiv -1 \cdot 2 \equiv 2 \pmod{4}.$$

Thus the set of integer solutions is $\{2 + 4k \mid k \in \mathbb{Z}\}$.  

3
Exercise 4.4.9

- A linear congruence modulo 5 with no solutions is $5x + 1 \equiv 0 \pmod{5}$.
- A linear congruence modulo 6 with no solutions is $3x + 1 \equiv 0 \pmod{6}$.
- A linear congruence modulo 6 with solution set $\{1 + 3k \mid k \in \mathbb{Z}\}$ is $2x - 2 \equiv 0 \pmod{6}$.

Exercise 5.1.10

Claim (a). Let $n \in \mathbb{Z}_{\geq 1}$. Then $2 + 4 + \cdots + 2n = n(n + 1)$.

Proof. Induction on $n$. The base case $n = 1$ is true since $2 = 1(1 + 1)$. Now suppose the claim is true for some $n = k \in \mathbb{Z}_{\geq 1}$, namely that $2 + 4 + \cdots + 2k = k(k + 1)$. Then $2 + 4 + \cdots + 2k + 2(k + 1) = k(k + 1) + 2(k + 1) = (k + 1)(k + 2)$, so the claim is true for $n = k + 1$. Thus we are done by induction.

Claim (b). Let $n \in \mathbb{Z}_{\geq 1}$. Then

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n + 1) = \frac{n(n + 1)(n + 2)}{3}.$$ 

Proof. Induction on $n$. The base case $n = 1$ is true since $1 \cdot 2 = 1 = \frac{1 \cdot 2 \cdot 3}{3}$. Now suppose the claim is true for some $n = k \in \mathbb{Z}_{\geq 1}$, namely

$$1 \cdot 2 + 2 \cdot 3 + \cdots + k(k + 1) = \frac{k(k + 1)(k + 2)}{3}.$$ 

Then

$$1 \cdot 2 + 2 \cdot 3 + \cdots + k(k + 1) + (k + 1)(k + 2) = \frac{k(k + 1)(k + 2)}{3} + (k + 1)(k + 2)$$

$$= \frac{k(k + 1)(k + 2) + 3(k + 1)(k + 2)}{3}$$

$$= \frac{(k + 1)(k + 2)(k + 3)}{3},$$

so the claim is true for $n = k + 1$. Thus we are done by induction.

Claim (c). Let $n \in \mathbb{Z}_{\geq 1}$. Then

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}.$$ 

Proof. Induction on $n$. The base case $n = 1$ is true since $1^2 = 1 = \frac{1 \cdot 2 \cdot 3}{6}$. Now suppose the claim is true for some $n = k \in \mathbb{Z}_{\geq 1}$, namely

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k + 1)(2k + 1)}{6}.$$
Then
\[
1^2 + 2^2 + \cdots + k^2 + (k + 1)^2 = \frac{k(k + 1)(2k + 1)}{6} + (k + 1)^2
\]
\[
= \frac{k(k + 1)(2k + 1) + 6(k + 1)^2}{6}
\]
\[
= \frac{(k + 1)(2k^2 + k + 6k + 6)}{6}
\]
\[
= \frac{(k + 1)(k + 2)(2k + 3)}{6},
\]
which proves the claim is true when \( n = k + 1 \). Thus we are done by induction. \( \Box \)

Claim (d). Let \( n \in \mathbb{Z}_{\geq 1} \). Then \( 1 \cdot 3 + 2 \cdot 4 + \cdots + n(n + 2) = n(2n - 1)(2n + 1) \).

This claim is false! Counterexample: Let \( n = 2 \). Then \( 1 \cdot 3 + 2 \cdot 4 = 11 \), but \( 2 \cdot 3 \cdot 5 = 30 \).

**Exercise 5.1.11**

Claim (a). Let \( n \in \mathbb{Z}_{\geq 1} \). Then \( n^2 + n \equiv 0 \pmod{2} \).

*Proof.* Induction on \( n \). The base case \( n = 1 \) is true since \( 1^2 + 1 = 2 \equiv 0 \pmod{2} \). Now suppose the claim is true for some \( n = k \in \mathbb{Z}_{\geq 1} \), namely \( k^2 + k \equiv 0 \pmod{2} \). Then

\[
(k + 1)^2 + (k + 1) = (k^2 + k) + 2(k + 1) \equiv 0 + 0 \pmod{2},
\]
which proves the claim when \( n = k + 1 \). Thus we are done by induction. \( \Box \)

Claim (b). Let \( n \in \mathbb{Z}_{\geq 1} \). Then \( n^2 - n \equiv 0 \pmod{3} \).

This claim is false! Counterexample: Let \( n = 2 \). Then \( 2^2 - 2 = 2 \not\equiv 0 \pmod{3} \).