Math 425 Assignment 3

Purpose

- Assess objectives and additional exercises from sections 1.2 and 1.3, namely
  - Intro-4: Execute the division algorithm and Aryabhata's (Bézout's) algorithm.
  - Intro-5: Solve congruence equations.
  - Supplemental exercises Supp-6, Supp-7, and Supp-8.
- Build a strong foundation of creative critical thinking and proof-writing techniques.

Task

- Complete the exercises listed on the following page(s) of this document and submit your solutions as a pdf to Canvas.
- I strongly recommend you use LaTeX to typeset your proofs.
- You may work in groups but everyone should submit their own assignment written in their own words. Do NOT copy your classmates.
- Allowed resources: our textbook, classmates, your notes, videos linked in Canvas.
- Unacceptable resources: anything you find on an internet search. Do NOT use a homework help website (e.g., Chegg). Their solutions are often wrong or use incorrect context. I want you to practice making arguments that are yours. Take some ownership.

Criteria

All items will earn a score using the following scale:

- **Exceptional** - Solution is succinct, references the correct theorems and definitions, and is entirely correct.
- **Satisfactory** - Solution is nearly correct. It still references the correct theorems and definitions. It may be longer than necessary, have minor errors, or have some grammatical mistakes.
- **Unsatisfactory** - Solution has major errors, references content not covered in class or in the textbook, or is incomplete in some major way.

Recall from the syllabus

- If you earn either an **Exceptional** or **Satisfactory** mark on an objective exercise (labeled Intro-, Group-, or Ring-) then you may consider that item complete.
- If you earn an **Unsatisfactory** mark on a an objective exercise (labeled Intro-, Group-, or Ring-) then you have not yet completed this objective.

- You may submit a new attempt at completing that objective on a future Wednesday. You must select a new exercise listed under the given objective, you cannot resubmit a version you have attempted previously. The only limit you have on number of attempts is the number of exercises available for the objective.
- Some objectives will be completed through WeBWorK. You must access these through the course on Canvas. Once you earn full credit on the assignment with at most 5 attempts, then you will have completed that objective.
- If you earn an **Exceptional** mark on an additional exercise (labeled A-) then you will earn one point toward the fifteen total points in that section of your overall grade. You can consider the exercise complete.
- If you earn an **Satisfactory** mark on an additional exercise (labeled Supp-) then you will earn 0.5 points toward the fifteen total points in that section of your overall grade. You may submit a new attempt at this exercise on a future Wednesday. Unlike the objective exercises, you must submit an attempt at the exact same exercise rather than another in a similar theme.
- If you earn an **Unsatisfactory** mark on an additional exercise (labeled Supp-) then you will earn 0 points toward the fifteen total points in that section of your overall grade. You may submit a new attempt at this exercise on a future Wednesday. Unlike the objective exercises, you must submit an attempt at the exact same exercise rather than another in a similar theme.

(Intro-4) Access this exercise on WeBWorK using the link on Canvas. That is, find the assignment titled `Intro-4`. Once you open this assignment, there will be a link to WeBWorK. This link will bring you directly to the exercise. You will have 5 attempts to answer all questions for the exercise correctly. After those 5 attempts, a new problem will be generated and you can start a new attempt to complete the objective.

(Intro-5) Access this exercise on WeBWorK using the link on Canvas. That is, find the assignment titled `Intro-5`. Once you open this assignment, there will be a link to WeBWorK. This link will bring you directly to the exercise. You will have 5 attempts to answer all questions for the exercise correctly. After those 5 attempts, a new problem will be generated and you can start a new attempt to complete the objective.

Name: ______________________________

(Supp-6) Show that no integers of the form $k^2 + 1$ are a multiple of 7.

Hint: In the context of equivalence mod 7, this would be equivalent to saying *no integer k satisfies the congruence equation* $k^2 + 1 \equiv 0 \pmod 7$.

Name: ______________________________

(Supp-7) Use proof by induction to show that If $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$ all have inverses in $\mathbb{Z}_n$, show that the same is true for the product $\overline{a}_1\overline{a}_2 \cdots \overline{a}_m$ for all $m \geq 2$.

Proof. Let $n \geq 2$ be an integer. We use induction on the value of m.
Base Case: Let $m = 2$. Assume $\overline{a}_1$ and $\overline{a}_2 \in \mathbb{Z}_n$ have inverses.

Show that $\overline{a}_1\overline{a}_2$ has an inverse. Use the definition of inverse here.

Inductive Step: Let $k \geq 2$ be an integer. Assume the statement holds for $m = k$. Let $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{k+1} \in \mathbb{Z}_n$ all have inverses.

Use the base case and the inductive hypothesis to show that $\overline{a}_1\overline{a}_2 \cdots \overline{a}_{k+1}$ has an inverse. Again, use the definition of inverse.

$\square$

Name: ____

(Supp-8) Let a and n be integers with $n \geq 2$. Let $d = \gcd(a, n)$. Show that for any integer b, the equation $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$.

Hint: You'll probably want to use Aryabhata's (Bézout's) identity here.