Instructions. Answer each of the questions on your own paper, and be sure to show your work so that partial credit can be adequately assessed. There is a total of 70 points possible. Put your name on each page of your paper.

1. [**12 Points**] Let $m = 143$ and $n = 176$.
   (a) Calculate the greatest common divisor $d = \gcd(m, n)$.
   (b) Write d in the form $sm + tn$ for some integers s and t.

2. [**12 Points**] Use induction to prove **one** of the following. Take your pick. (Just make a direct induction proof. Do not assume any other facts about congruences or summation formulas.)
   (a) For any positive integer n, $n^3 + 5n$ is a multiple of 3.
   (b) For any positive integer n, $\sum_{k=1}^{n}(2k+1) = n(n+2)$.

3. [**10 Points**] Use properties of congruences to compute the following. Express your answers as the least residue $\pmod{n}$, that is, in the form $x \pmod{n}$ where $0 \le x < n$. Make the arithmetic as easy as possible.
   (a) $708 \cdot 75 \cdot 6999 \pmod 7$
   (b) $7^5 + (602)^5 \pmod 6$

4. [**12 Points**] Short answer questions.
   (a) Fill in the blanks to complete the statement of the division algorithm: Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that
   $\boxed{}$ where $\boxed{}$.
   (b) Euclid's Lemma states: Let a and b be integers and let p be a $\boxed{}$ number.
   If $p \mid ab$, then $\boxed{}$.
   (c) **T**rue or **F**alse. If, for nonzero integers a, b, d, there are integers x and y with $ax+by = d$, then d is the greatest common divisor of a and b.
   (d) Define a binary operation $\circ$ on the integers $\mathbb{Z}$ to be ordinary subtraction. That is, $a \circ b = a - b$. Is 0 an identity element for the binary operation $\circ$? Explain.

5. [**12 Points**] Define a relation $\sim$ on $\mathbb{Z}_8$ by $x \sim y$ if $x^2 = y^2$, where $x, y \in \mathbb{Z}_8$.
   (a) Verify that $\sim$ is an equivalence relation on $\mathbb{Z}_8$.
   (b) Find all of the distinct equivalence classes for the equivalence relation $\sim$.

6. [**12 Points**] Let $G_1 = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$ and $G_2 = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, c \in \mathbb{R}, ac \neq 0, b \in \mathbb{Z} \right\}$.
   (a) Show that G_1 is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.
   (b) Show that G_2 is not a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Bonus (10 Points) If G is a group with $x^2 = e$ for all $x \in G$, where e is the identity, prove that G is abelian.