Instructions. Answer each of the questions on your own paper. Be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. [**20 Points**] Solve the congruence $6x \equiv 27 \mod 69$.

2. [**16 Points**] Compute $[91]_{501}^{-1}$ in $\mathbb{Z}_{501}^*$. Recall that $\mathbb{Z}_n^*$ denotes the congruence classes of integers modulo n that have a multiplicative inverse modulo n.

3. [**22 Points**] Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 3 & 7 & 5 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 6 & 7 & 1 & 5 \end{pmatrix}$ in S_7.

   (a) Compute $\sigma\tau$, $\tau\sigma$ and σ^{-1} in two-rowed notation.

   (b) Write each of σ, τ, $\sigma\tau$ and $\tau\sigma$ as a product of disjoint cycles.

   (c) Compute the order in the group S_7 of each of the elements σ, τ, $\sigma\tau$ and $\tau\sigma$.

4. [**20 Points**] Let G be a group.

   (a) State the definition of a *subgroup* of G.

   (b) State a result that tells you which conditions to check when determining whether or not a subset H of G is a subgroup of G. Use this result in proving part (c).

   (c) Let H and K be subgroups of G. Prove that $H \cap K = \{g \in G \mid g \in H \text{ and } g \in K\}$ is a subgroup of G.

5. [**20 Points**] For each of the following statements, either indicate that the statement is true (no proof required), or give a counterexample if the statement is false. You must justify that your counterexample is in fact a counterexample.

   (a) If G is a group of order n, then $x^n = e$ for every $x \in G$.

   (b) If G is a group of order n, then every element (except the identity) has order n.

   (c) If G is a group of order n, then there is at least one element of G which has order n.

   (d) If a and b are elements of G of order m and n, respectively, then the element ab has order $[m, n]$, the least common multiple of m and n.

6. [**16 Points**] Do ONE of the following problems.

   (a) Let $G = \mathbb{Z}_{11}^*$. Show that G is cyclic, find all of the subgroups of G, and give the subgroup diagram which shows the inclusions between them.

   (b) Show that the three groups $\mathbb{Z}_6$, $\mathbb{Z}_9^*$ and $\mathbb{Z}_{18}^*$ are isomorphic to each other.

7. [**18 Points**] Let $G = \langle a \rangle$ be a cyclic group of order 8 with generator a, with the group operation written multiplicatively, and let $H = \mathbb{Z}_2 \times \mathbb{Z}_4$, the cartesian product of $\mathbb{Z}_2$ and $\mathbb{Z}_4$. Remember that the group operation on the group $\mathbb{Z}_n$ is addition of congruence classes.

   (a) Complete the following table so as to make the function $f : G \to H$ a homomorphism. (*Hint:* Use the fact that a homomorphism satisfies $f(a^2) = f(a)f(a)$, $f(a^3) = f(a^2)f(a)$, etc. and remember that product means group operation.)

g	e	a	a^2	a^3	a^4	a^5	a^6	a^7
$f(g)$	$([0]_2,\ [0]_4)$	$([1]_2,\ [3]_4)$						

   (b) Find the kernel of f. (Recall that $\mathrm{Ker}(f) = \{x \in G : f(x) = e'\}$, where e' is the identity of the group H.)

   (c) Find the image of f. (Recall that $\mathrm{Im}(f) = \{y \in H : y = f(x) \text{ for some } x \in G\}$.)

8. [**18 Points**] Let F be a field.

   (a) State the division algorithm for polynomials in $F[x]$.

   (b) Use the division algorithm to find the quotient and remainder when $f(x) = 2x^4 + x^3 + x^2 + 6x + 2$ is divided by $g(x) = 2x^2 + 2$ over the field $\mathbb{Z}_7$.

   (c) List all of the irreducible polynomials over $\mathbb{Z}_2$ of degree 2. Justify that your list is complete.