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. **[15 Points]** Solve the congruence $5x \equiv 23 \mod 32$.

   ▶ **Solution.** Since $\gcd(5, 32) = 1$, there is a unique solution modulo 32. By the Euclidean algorithm (or by inspection) $5 \cdot 13 - 2 \cdot 32 = 1$, so that $[5]_{32}^{-1} = [13]_{32}$. Hence, $5x \equiv 23 \mod 32 \iff$

   $$\begin{aligned} x &\equiv 13 \cdot 23 \mod 32 \\ &\equiv 299 \mod 32 \\ &\equiv 11 \mod 32. \end{aligned}$$

   Thus, $x = 11 + 32k$ for $k \in \mathbb{Z}$. ◀

2. **[15 Points]** Let $\alpha = (3, 1, 7, 5, 9)$, $\beta = (6, 2, 8, 4)$ and $\sigma = \alpha\beta$ in S_9.

   (a) What are the orders of α, β and σ?

   ▶ **Solution.** Since α and β are disjoint cycles, of length 5 and 4, respectively, $o(\alpha) = 5$, $o(\beta) = 4$, and $o(\sigma) = \text{lcm}[5, 4] = 20$. ◀

   (b) Find the smallest positive integer m such that $\sigma^m = \alpha$.

   ▶ **Solution.** Since α and β are disjoint permutations, they commute. Hence $\sigma^m = (\alpha\beta)^m = \alpha^m\beta^m = \alpha$ provided that $m \equiv 1 \mod 5$ and $m \equiv 0 \mod 4$. Solving this simultaneous congruence gives $m \equiv 16 \mod 20$. The smallest positive solution is thus $m = 16$. ◀

   (c) Find *all* of the integers m such that $\sigma^m = \alpha$.

   ▶ **Solution.** If $\sigma^m = \sigma^n = \alpha$, then $m \equiv n \mod o(\sigma)$. Hence $m \equiv 16 \mod 20$. ◀

3. **[30 Points]** Let $G = \mathbb{Z}_{16}^* = \{[r] \in \mathbb{Z}_{16} : \gcd(r, 16) = 1\}$. Recall that $\mathbb{Z}_{16}^*$ is a group under the operation of multiplication modulo 16. Let $H = \langle[7]\rangle$ be the cyclic subgroup of G generated by $[7]$ and let $K = \langle[9]\rangle$ be the cyclic subgroup of G generated by $[9]$.

   (a) List the elements of G, the elements of H and the elements of K.

   ▶ **Solution.** $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $H = \{1, 7\}$ (since $7^2 = 49 \equiv 1 \mod 16$), and $K = \{1, 9\}$ (since $9^2 \equiv 1 \mod 16$). ◀

   (b) Are H and K isomorphic groups?

   ▶ **Solution.** Both are cyclic groups of order 2, and hence are isomorphic. ◀

(c) List all of the distinct cosets of H in G.

► **Solution.** $H = \{1, 7\}$, $3H = \{3, 5\}$, $9H = \{9, 15\}$, $11H = \{11, 13\}$. ◄

(d) List all of the distinct cosets of K in G.

► **Solution.** $K = \{1, 9\}$, $3K = \{3, 11\}$, $5K = \{5, 13\}$, $7K = \{4, 15\}$. ◄

(e) Write the multiplication table for G/H.

► **Solution.**

$\cdot$	H	$3H$	$9H$	$11H$
H	H	$3H$	$9H$	$11H$
$3H$	$3H$	$9H$	$11H$	H
$9H$	$9H$	$11H$	H	$3H$
$11H$	$11H$	H	$3H$	$9H$

◄

(f) Write the multiplication table for G/K.

► **Solution.**

$\cdot$	K	$3K$	$5K$	$7K$
K	K	$3K$	$5K$	$7K$
$3K$	$3K$	K	$7K$	$5K$
$5K$	$5K$	$7K$	K	$3K$
$7K$	$7K$	$5K$	$3K$	K

◄

(g) By inspecting your multiplication tables determine if the two factor groups G/H and G/K are isomorphic. Be sure to explain, by specific references to the tables, how you arrived at your conclusion.

► **Solution.** G/H is a cyclic group of order 4 with generator $a = 3H$, since $a^2 = 9H$, $a^3 = 11H$, $a^4 = H$ =identity of G/H, while every element of G/K has order 1 or 2 since $b^2 = K$ =identity of G/K for all elements b of G/K. ◄

4. **[30 Points]** Each of the following statements may be either **True** or **False**. Determine which and give a brief reason why.

(a) If G is a group with 13 elements, then the only subgroups of G are the identity subgroup $\{e\}$ and the entire group G itself.

► **Solution. True.** By Lagrange's Theorem any subgroup H of G has order dividing $|G| = 13$. Since 13 is prime, this means that $|H| = 1$ or 13. If $|H| = 1$, then $H = \{e\}$, and if $|H| = 13$, then $H = G$. ◄

(b) If G is a group of order $|G| = 15$ and H is a subgroup with $|H| = 3$, then every coset of H in G has 5 elements.

▶ **Solution. False.** Each coset has the same number of elements as H, that is, 3. ◀

(c) If $\sigma \in S_6$, then the order of σ divides 6.

▶ **Solution. False.** $\sigma = (1, 2, 3, 4) \in S_6$ and $o(\sigma) = 4$, which does not divide 6. ◀

(d) The polynomial $p(x) = x^5 + 12x^3 + 6x^2 - 24x + 18$ is irreducible in $\mathbb{Q}[x]$.

▶ **Solution. True.** Apply Eisenstein's criterion with the prime $p = 2$. ◀

(e) There are polynomials $p(x)$ and $q(x) \in \mathbb{Z}_5[x]$ such that

$$p(x)(x^5 - 2x^3 + 4) + q(x)(x^2 - 1) = 1.$$

▶ **Solution. False.** Suppose there were such an equation. Substitute $x = -1$. This gives an identity $0 = 1$, which is a contradiction. ◀

(f) $\mathbb{Z}_{47}$ is a field.

▶ **Solution. True.** Apply the theorem that states that $\mathbb{Z}_n$ is a field if and only if n is prime. Since 47 is prime, it follows that $\mathbb{Z}_{47}$ is a field. ◀

5. **[15 Points]** Let G be a group such that $x^2 = e$ for every $x \in G$. Prove that G is abelian.

▶ **Solution.** Let a and b be arbitrary elements of G and let $x = ab \in G$. Then $x^2 = e$, so that $(ab)(ab) = e$. Multiply this equation on the left by a and on the right by b to get $a^2bab^2 = aeb = ab$. But $a^2 = b^2 = e$ so we conclude that $ba = ebae = a^2bab^2 = ab$, and hence G is abelian. ◀

6. **[15 Points]** Let $G = \mathbb{Z}_7^*$.

(a) Show that G is a cyclic group by finding a generator.

▶ **Solution.** $|\mathbb{Z}_7^*| = 6$ and $3^2 = 9 \equiv 2 \mod 7$ and $3^3 \equiv 6 \mod 7$. Hence, $o(3)|6$ but $\phi(3) \neq 2$ and $o(3) \neq 3$. Hence $o(3) = 6$ and $\mathbb{Z}_7^* = \langle 3 \rangle$. ◀

(b) List *all* of the subgroups of G.

▶ **Solution.** Since $\mathbb{Z}_7^*$ is cyclic of order 6, there is exactly one subgroup of $\mathbb{Z}_7^*$ of each order dividing 6. Thus, the subgroups are:

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 2 \rangle &= \{1, 2, 4\} \\ \langle 6 \rangle &= \{1, 6\} \\ \langle 3 \rangle &= \mathbb{Z}_7^*. \end{aligned}$$

◀

7. **[15 Points]** Let $E = \mathbb{Q}[x]/\langle x^2 - 5\rangle$ be the set of congruence classes of polynomials modulo $x^2 - 5$. As usual, we will denote the congruence class of $p(x) \in \mathbb{Q}[x]$ by the symbol $[p(x)]$.

   (a) Explain briefly why $E = \mathbb{Q}[x]/\langle x^2 - 5\rangle$ is a field.

   ▶ **Solution.** If F is a field, then the congruence class space $F[x]/\langle p(x)\rangle$ is a field if and only if $p(x)$ is irreducible over F. Since $x^2 - 5$ is irreducible over $\mathbb{Q}$ (by either the rational root theorem or Eisenstein's criterion with $p = 5$), it follows that E is a field. ◀

   (b) Find a and b in $\mathbb{Q}$ so that $[x^3 - 2x^2 - 4x + 12] = [a + bx]$.

   ▶ **Solution.** In E, $[x^2 - 5] = [0]$, so $[x^2] = [5]$ and $[x^3] = [5x]$. Hence,

   $$[x^3 - 2x^2 - 4x + 12] = [5x - 2 \cdot 5 - 4x + 12] = [x = 2].$$

   Alternatively, one can use long division to get

   $$x^3 - 2x^2 - 4x = 12 = (x^2 - 5)(x - 2) + (x + 2),$$

   which gives $[x^3 - 2x^2 - 4x + 12] = [x + 2]$. ◀

   (c) Find the multiplicative inverse of $[x^3 - 2x^2 - 4x + 12]$ in E.

   ▶ **Solution.** Either use the Euclidean algorithm, or notice that $(x^2-5)+1 = x^2-4 = (x+2)(x-2)$. Hence, in E, $[x+2][x-2] = [1]$ so that $[x = 2]^{-1} = [x-2]$. ◀

8. **[15 Points]** Let $G = \langle a\rangle$ be a cyclic group of order 9 with generator a and let $H = S_3$.

   (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.)

g	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
$f(g)$	(1)	(1, 2, 3)							

   ▶ **Solution.**

g	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
$f(g)$	(1)	(1, 2, 3)	(1, 3, 2)	(1)	(1, 2, 3)	(1, 3, 2)	(1)	(1, 2, 3)	(1, 3, 2)

   ◀

   (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.)

   ▶ **Solution.** $\mathrm{Ker}(f) = \{1, a^3, a^6\}$ ◀

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

   ▶ **Solution.** $\mathrm{Im}(f) = \{(1), (1, 2, 3), (1, 3, 2)\}$ ◀