1. (a) For positive integers a and b, define $\gcd(a, b)$.

   (b) Compute $\gcd(1776, 1492)$.

   (c) Show that if a, b, c are positive integers, then $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

2. (a) Find $\varphi(32)$.

   (b) Use the Euclidean algorithm to find $[5]_{32}^{-1}$ in $\mathbf{Z}_{32}^{\times}$.

   (c) Find all powers of $[5]_{32}$ in $\mathbf{Z}_{32}^{\times}$.

3. Define $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 3 & 2 & 5 & 7 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 6 & 7 & 1 & 5 \end{pmatrix}$.

   (a) Compute $\sigma\tau$ and $\tau\sigma$.

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

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

4. Let S be the set of all ordered pairs (m, n) of positive integers m, n. On S, define $(m_1, n_1) \sim (m_2, n_2)$ if $m_1 + n_2 = m_2 + n_1$.

   (a) Show that $\sim$ defines an equivalence relation on S.

   (b) On the equivalence classes $S/\sim$, define an addition as follows:

   $[(m_1, n_1)] + [(m_2, n_2)] = [(m_1 + m_2, n_1 + n_2)]$.

   Show that there is an identity element for this addition. Then find a formula for the additive inverse of $[(m, n)]$. (You may assume that the formula for addition gives a well-defined and associative binary operation.)

5. (a) State these definitions: *group*; *subgroup*.

   (b) State Lagrange's theorem.

   (c) Let G be a group, and let H be a nonempty subset of G. Suppose that if x and y are any elements of H, then $xy^{-1} \in H$. Show that H must be a subgroup of G.

6. Let m and n be positive integers with $\gcd(m, n) = 1$.

   Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$, for all $[x]_{mn} \in \mathbf{Z}_{mn}$.

   (a) Show that ϕ is a well-defined function.

   (b) State the definition of an isomorphism of groups.

   (c) Show that ϕ is an isomorphism.

7. For each of the following, either indicate that the statement is true, or give a counterexample if the statement is false.

   (a) If G is a finite group of order n, then every element x of G satisfies the equation $x^n = e$.

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

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

   (d) If G is a finite group of order n, and n is prime, then there is at least one element of G that has order n.

   (e) If a and b are group elements of order m and n, respectively, then the element ab has order $\mathrm{lcm}[m, n]$.

8. Prove **ONE** of the following theorems from the text.

   I. Every subgroup of a cyclic group is cyclic.

   II. If G is a cyclic group of order n, then G is isomorphic to $\mathbf{Z}_n$.

   III. Every group is isomorphic to a group of permutations.

1. Solve the following system of congruences:

$$2x \equiv 9 \pmod{15} \qquad x \equiv 8 \pmod{11}$$

2. Find $[91]_{501}^{-1}$ (in $\mathbf{Z}_{501}^{\times}$).

3. Let $\sigma = (2,4,9,7,)(6,4,2,5,9)(1,6)(3,8,6) \in S_9$.

   (i) Write σ as a product of disjoint cycles.

   (ii) What is the order of σ?

   (iii) Compute σ^{-1}.

4. 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 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. (a) State the definition of a cyclic group.

   (b) Write out ONE of the following proofs from the text:

   I. Any subgroup of a cyclic group is cyclic.

   II. If G is a cyclic group of order n, then G is isomorphic to $\mathbf{Z}_n$.

6. Do ONE of the following problems.

   I. Find all subgroups of $\mathbf{Z}_{11}^{\times}$, and give the lattice diagram which shows the inclusions between them.

   II. Show that the three groups $\mathbf{Z}_6$, $\mathbf{Z}_9^{\times}$, and $\mathbf{Z}_{18}^{\times}$ are isomorphic to each other.

7. Let G be the subgroup of $\mathrm{GL}_3(\mathbf{R})$ consisting of all matrices of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ such that } a, b \in \mathbf{R}\ .$$

   Show that G is a subgroup of $\mathrm{GL}_3(\mathbf{R})$.

8. Show that the group G in problem 7 is isomorphic to the direct product $\mathbf{R} \times \mathbf{R}$.

1. (20 pts) Find $\gcd(980, 189)$ and express it as a linear combination of 980 and 189.

2. (20 pts)

   (a) Is $7^{123} + 1$ divisible by 3?

   (b) What is the last digit in the decimal expansion of 4^{123}?

3. (20 pts) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 3 & 1 & 4 & 7 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 6 & 5 & 4 & 3 \end{pmatrix}$.

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

   (b) Find the order of each of σ, τ, $\sigma\tau$, and $\tau\sigma$.

4. (20 pts) Define $f : \mathbf{Z}_n \to \mathbf{Z}_m$ by $f([x]_n) = [kx]_m$. Show that the formula f defines a function if and only if $m \mid kn$. Find conditions on n, m, k that determine when f is a one-to-one correspondence.

5. (20 pts) Let G be a group and let H be a subgroup of G. For elements $x, y \in G$, define $x \sim y$ if $y^{-1}x \in H$. Check that $\sim$ defines an equivalence relation on G.

6. (25 pts)

   (a) Define the following terms: group; cyclic group; order of an element of a group.

   (b) State the following theorems: Lagrange's theorem (about the order of a subgroup); Cayley's theorem (about groups of permutations).

7. (25 pts) Let G be any cyclic group. Prove that G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some positive integer n.

8. (20 pts)

   (a) Show that $\mathbf{Z}_5^\times$ is isomorphic to $\mathbf{Z}_{10}^\times$.

   (b) Show that $\mathbf{Z}_{30}^\times$ is *not* isomorphic to $\mathbf{Z}_{24}^\times$.

9. (30 pts) Let G and G' be groups, and let $\phi : G \to G'$ be a function (not required to be either one-to-one or onto) such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

   (a) Let e and e' denote the identity element of G and G'. Show that $\phi(e) = e'$, and that $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$.

   (b) Show that the subset $\{g \in G \mid \phi(g) = e'\}$ is a subgroup of G.

   (c) Show that the subset $\{y \in G' \mid y = \phi(x) \text{ for some } x \in G\}$ is a subgroup of G'.

MATH 420 FINAL EXAM, J. Beachy, 12/12/90

Answer any eight questions.

1. Let a and b be nonzero integers. Prove that $(a,b) = 1$ if and only if $\gcd(a+b, ab) = 1$.

2. Solve the following system of congruences:

$$2x \equiv 7 \pmod{15} \qquad 3x \equiv 5 \pmod{14}$$

3. Let G be any cyclic group. Prove that G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some positive integer n.

4. Let G be a group and let H be a subgroup of G. For any element $a \in G$, define

$$Ha = \{x \in G \mid x = ha \text{ for some } h \in H\} .$$

Prove that the collection of all such subsets partitions G.

5. Let $\sigma = (2,4,9,7,)(6,4,2,5,9)(1,6)(3,8,6) \in S_9$.

(i) Write σ as a product of disjoint cycles.

(ii) What is the order of σ?

(iii) Compute σ^{-1}.

6. Let G be a group. Show that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

7. If a nontrivial group G has no proper nontrivial subgroups, prove that G is cyclic and that the order of G is a prime number.

8. Let G be any group. In the proof of Cayley's theorem, for each $a \in G$ a function $\lambda_a : G \to G$ is defined by $\lambda_a(x) = ax$, for all $x \in G$.

(a) Prove that λ_a is a permutation of G, for any $a \in G$.

(b) Prove that $\{\lambda_a \mid a \in G\}$ is a subgroup of $\mathrm{Sym}(G)$.

9. Let G be a group and let H and K be subgroups of G. Prove that $H \cap K$ is a subgroup of G.

10. Define the following terms: one-to-one function; onto function; group; cyclic group.

1. (30)

   (a) State the Division Algorithm.

   (b) State the definition of one-to-one function; onto function.

   (c) State the definition of a group.

2. (20) Let G, G' be groups, and let $\phi : G \to G'$ be a function such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. Prove that
$$K = \{x \in G \mid \phi(x) = e\}$$
   is a subgroup of G.

3. (15) Define a function ϕ from the multiplicative group $C^\times$ of complex numbers into itself by $\phi(a+bi) = a - bi$. Prove that ϕ is an isomorphism.

4. (35)

   (a) State the proposition which gives the solution to all linear congruences of the form $as \equiv b \pmod{n}$.

   (b) State the proposition which tells how to compute the order of any element in a cyclic group of order n.

   (c) For the special case of the cyclic group $\mathbf{Z}_n$, show that the result in (a) can be used to prove (b).

5. (30) Let N be a subgroup of the group G.

   (a) For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in N$. Show that $\sim$ defines an equivalence relation.

   (b) Assume that $gxg^{-1} \in N$ for all $x \in N$ and $g \in G$. Prove that if $a \sim b$ and $b \sim d$, then $ab \sim cd$.

   Hint: Show that if $ac^{-1} \in N$ and $bd^{-1} \in N$, then $ac^{-1}cbd^{-1}c^{-1} \in N$.

6. (25) State and prove Lagrange's Theorem. OR State and prove Cayley's Theorem.

7. (25) Let G be the set of matrices of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, where $a, b, c \in \mathbf{Z}_2$. Prove that G is a group.

   Is it abelian? Is it cyclic? Compute the order of each of its elements.

8. (20) Prove that if $\gcd(m, n) = 1$, then $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$.

MATH 420 FINAL EXAM J. Beachy, 12/18/87

Each problem is worth 25 points.

1. Write out the definitions of the following concepts:
   (a) group
   (b) cyclic group
   (c) one-to-one function; onto function
   (d) greatest common divisor of two integers.
2. Write out the statements of the following theorems:
   (a) The Division Algorithm
   (b) Lagrange's Theorem (on the order of a subgroup of a finite group)
   (c) The theorem which gives $\varphi(n)$ in terms of the prime factorization of n.
3. Write out the proof of the theorem which states that every subgroup of a cyclic group is cyclic.
4. Write out a proof of Cayley's Theorem, which states that every group is isomorphic to a group of permutations.
5. Let a, b, d, m, n be integers. If $\gcd(a, b) = d$ and $an + bm = d$, then prove that $\gcd(n, m) = 1$.
6. Let $\sigma = (2, 8, 5)(5, 7, 8)(3, 8)(8, 6)$ in S_9. Write σ as a product of disjoint cycles. What is the order of σ? Compute σ^{-1}.
7. For real numbers a, b we define $a \sim b$ if $a - b$ is an integer. Show that $\sim$ is an equivalence relation of the set of real numbers.
8. Show that the set $G = \left\{ \left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right] \middle| x \in \mathbf{R} \right\}$ is a group under matrix multiplication, and show that G is isomorphic to $\mathbf{R}$, the group of all real numbers under addition.