Math 453
Fall 2011
Exam II Solution

Instructions: Give a complete solution to each problem. Be sure you make clear reference to each fact that you are citing. Write complete sentences and be sure to work the problems in an order that will maximize your score.

1. **(3 points each)** For each of the following terms, give a precise definition;

   (a) Even Permutation.

   (b) Cyclic group

   (c) Right Coset of a subgroup H is a group G.

   (d) Isomorphism.

   Solution:

   (a) A permutation is **even** if it can be expressed as a product of an even number of 2–cycles.

   (b) A group, G, is **cyclic** if $G = \{a^n | n \in \mathbb{Z}\}$, for some $a \in G$.

   (c) A **right coset** of a subgroup H of G is a set of the form $Ha = \{ha | h \in H\}$, for some $a \in G$.

   (d) An **isomorphism** between groups is a function $\varphi : G \to \bar{G}$ which is one-to-one, onto, and satisfies $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a, binG$.

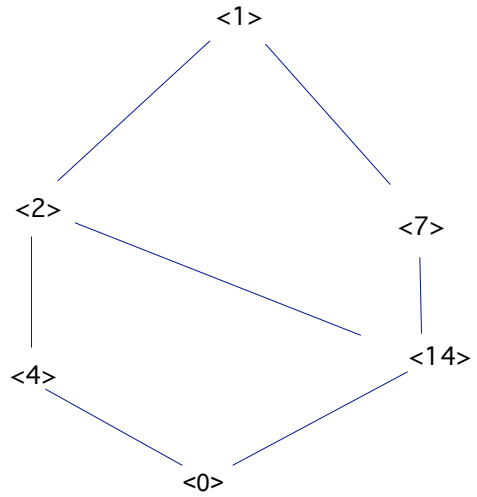
2. **(8 points each)**

   (a) Draw the subgroup lattice for $\mathbb{Z}_{28}$.

   (b) Find all elements of order 14 in $\mathbb{Z}_{84}$. (**Hint:** Start with an "obvious" element of order 14, and then determine the relation of all other such elements to this one.)

   Solution:

   (a) Since the divisors of 28 are $1, 2, 4, 7, 14$, and 28 the Fundamental Theorem of cyclic Groups says there is a unique subgroup of each of these orders, that these are the only subgroups. Moreover, if $d|28$, then the unique subgroup of order d is given by $\langle n/d \rangle$,and if $\langle d_1 \rangle \subset \langle d_2 \rangle$ if and only if $d_2|d_1$. Thus, the lattice of subgroups is



(b) Since $14|84$, we know $\mathbb{Z}_{84}$ has a subgroup of order 14, generated by $84/14 = 6$. Thus, $|6| = 14$. Moreover, the elements of order 14 in $\mathbb{Z}_{84}$ are of the form $6k$, with $k]inU(14)$. Since $U(14) = \{1, 3, 5, 9, 11, 13\}$, and thus $6, 18, 30, 54, 66$, and 78 are the elements of $\mathbb{Z}_{84}$ of order 14.□

3. **(16 points)** Let $\varphi : G \to \bar{G}$ be an isomorphism. Show, using some form of mathematical induction, $\varphi(a^n) = (\varphi(a))^n$, for all $a \in G$ and all $n \geq 1$.

   Proof: For $n = 1$, we have $\varphi(a^1) = \varphi(a) = (\varphi(a))^1$, so the claim holds for $n = 1$. Now suppose, for some $n \geq 1$, we have $\varphi(a^n) = (\varphi(a))^n$. Now, note $\varphi(a^{n+1}) = \varphi(a^n a) = \varphi(a^n)\varphi(a)$, since φ is an isomorphism. Now, by our inductive hypothesis, we have

   $$\varphi(a^{n+1}) = \varphi(a^n)\varphi(a) = (\varphi(a))^n\varphi(a) = (\varphi(a))^{n+1}.$$

   Therefore, by the first principle of mathematical induction, we have $\varphi(a^n) = (\varphi(a))^n$, for all $a \in G$ and all $n \geq 1$.□

4. Let $\alpha \in S_8$ be given by $\alpha = (1287)(2375)(1634)(253)$.

   (a) **(6 points)** Write α as a product of disjoint cycles.

   (b) **(4 points)** Is $\alpha \in A_8$?? Why or why not?

   Solution:

   (a) We compute directly, $\alpha = (16)(28754)$.

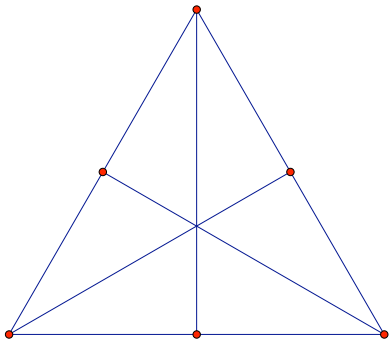
   (b) We note α is the product of an odd permutation, (16), and an even permutation (28754), and thus is an odd permutation. Hence $\alpha \notin A_8$.□

5. **(8 points)** Compute $3^{123} \bmod 11$

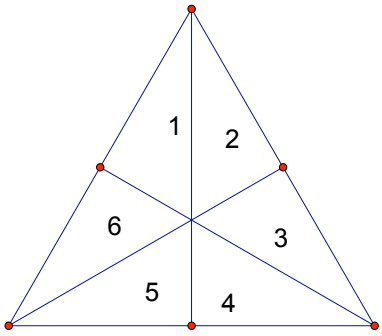
Solution: By Fermat's Little Theorem, we have $a^p \equiv a \bmod p$, for any prime p and every $a \in \mathbb{Z}$. Thus, $3^{11} \equiv 3 \bmod 11$. Thus,

$$3^{123} = 3^{121+2} = (3^{11})^{11}3^2 \equiv 3^{11}3^2 \equiv 3^3 \equiv 5 \bmod 11. \square$$

6. **(18 points)** Consider an equilateral triangle subdivided into six right triangles by the lines of reflection for its symmetry group, D_3. (See the figure below.) Recall two colorings are equivalent if there is a φ in D_3 which takes one to the other. Determine an equation for the number of non-equivalent colorings of this figure using four colors.



Solution: We number the triangular cells as in the picture,



Now, $G = D_3$ acts on the figure by rotations and reflections. There are 4^6 possible arrangements of the colorings (four choices for each of the 6 cells). Now the identity R_0 fixes all 4^6 arrangements. There are two rotations of order 3, namely R_{120} and R_{240}. We see if an arrangement is fixed under R_{120}, then cells $1, 3$, and 5 must be the same color and cells $2, 4$, and 6 must be the same color. Therefore, there are 4^2 such colorings. There are 3 elements of order 2, namely the reflections. For the reflection F through the vertex shared by cells 1 and 2, we see a coloring is fixed by F if cells 1 and 2 are the same color, cells 3, and 6 are the same color, and cells

4 and 5 are the same color. Thus, there are 4^3 such colorings. Now, by Burnside's Lemma, there are

$$\frac{1}{|G|}\sum_{\varphi\in G}|\operatorname{fix}(\varphi)| = \frac{1}{6}(4^6 + 2\cdot 4^2 + 3\cdot 4^3).\square$$

Note, this is, in fact, 720 different colorings.

7. **TRUE/FALSE (5 points each)** For each of the statements below, decide whether the statement is true or false. If it is true then justify it by proving it or citing a theorem. If it is false then give a specific counterexample.

   (a) Any function $\varphi : G \to G$ which is one-to-one and onto is an isomorphism.

   (b) If p and q are unequal primes and G is a group of order pq, then any proper subgroup of G is cyclic.

   (c) For any group G, any subgroup H of G and any $a \in G$, $Ha = aH$.

   (d) If $\operatorname{Aut}(G) \cong \operatorname{Aut}(H)$ then $G \cong H$.

   Solution:

   (a) **False:** Consider $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2$ given by $\varphi(0) = 1, \varphi(1) = 0$. This function is one-to-one and onto, but is not an isomorphism, because $\varphi(0)$ is not the identity of the group $\mathbb{Z}_2$.

   (b) **True:** Any proper subgroup has order $1, p$, or q, by Lagrange's Theorem. Since any group of prime order is cyclic, and the trivial group is cyclic, any proper subgroup of a group of order pq is cyclic.

   (c) **False:** Consider $G = S_3$, $H = \{\varepsilon, (12)\}$, and $a = (123)$. Then

   $$Ha = \{(123), (12)(123)\} = \{(123), (23)\},$$

   while

   $$aH = \{(123), (123)(12)\} = \{(123), (13)\} \neq Ha.$$

   (d) **False:** We have $\operatorname{Aut}(\mathbb{Z}_{10}) \cong U(10) \cong \mathbb{Z}_4 \cong U(5) \cong \operatorname{Aut}(\mathbb{Z}_5)$. But $\mathbb{Z}_{10} \ncong \mathbb{Z}_5$.$\square$

Extra Credit: (10 points) Suppose G is a group of odd order. Prove the equation $x^2 = a$ has a unique solution for each $a \in G$.

Solution: Let $|G| = 2n + 1$, for some $n \geq 0$. By a corollary to Lagrange's Theorem $a^{|G|} = e$ for any $a \in G$. So $a^{2n+2} = a$. Suppose $x^2 = y^2$ for some $x, y \in G$. Then $x = x^{2n+2} = (x^2)^{n+1} = (y^2)^{n+1} = y^{2n+2} = y$. Thus, the map $\varphi : G \to G$ given by $\varphi(x) = x^2$ is one-to-one. Thus, since G is finite φ is also onto. Therefore, for each $a \in G$, there is a unique $x \in G$ with $x^2 = a$.$\square$.