Problem Set 4  (Solutions are due Wed. 2-27-08)

1) A popular method to generate pseudo-random numbers on a computer is the linear congruential method. Starting with a seed \( x_0 \), the sequence of pseudo-random numbers \( \{x_i\}_{i \geq 0} \) is generated recursively by
\[
x_{i+1} = a x_i + c \pmod{n}, \quad a, c, n \text{ fixed integers}.
\]

Given the following two sequences which were obtained using the above recursion, determine in both cases \( a, c, n \) and the next \( x_i \) in the sequence if this is possible at all. Otherwise explain why it is not possible.

(a) \( \{x_i\}_{i \geq 0} = \{206, 207, 180, 141, 170, 155, 48, 121, \ldots\} \).

(b) \( \{x_i\}_{i \geq 0} = \{50300, 81383, 8326, 12329, 78592, 76315, 38698, \ldots\} \).

2) Consider the ring of integers \( \mathbb{Z}_{39} \) and its multiplicative subgroup \( \mathbb{Z}_{39}^\times \).

(a) Determine which of the following subsets \( H_i \) of \( \mathbb{Z}_{39}^\times \) are groups \( \langle H_i, \ast \rangle \) under the operation of multiplication modulo 39:
\[
H_1 = \{1, 4, 10, 16, 22, 25\}, \quad H_2 = \{1, 8, 17\}, \quad H_3 = \{1, 2, 4, 5, 8, 10, 11, 16, 20, 22, 25, 32\}, \quad H_4 = \{1, 4, 10, 14, 16, 17, 22, 23, 25, 29, 35, 38\}, \quad H_5 = \{1, 16, 17, 22, 23, 29, 38\}, \quad H_6 = \{1, 4, 7, 10, 16, 19, 22, 25, 28, 31, 34, 37\}.
\]

(b) Two groups \( \langle G, \ast \rangle \) and \( \langle G', \times \rangle \) are said to be isomorphic if there is a one-to-one mapping \( g' = f(g) \) between the elements of the two groups which preserves the group operation, i.e., if
\[
f(g_i \ast g_j) = f(g_i) \times f(g_j), \quad \text{for all } i, j.
\]

Two of the groups in (a) are isomorphic. Determine which.

3) **Groups, Generators, and their Graphs**. Groups, even if they have the same number of elements, can have very different properties. One way to visualize this is to draw a graph of the group. Start with a generator element or a generator set and draw all possible paths that lead from the identity element to other elements. Then draw all paths that lead to further elements by using the group operation and the generator element(s) repeatedly. If the group is finite, the process eventually stops because no more new elements are generated. Here are three examples of groups of size 6:
Example 1: Consider the set of elements \( G = \{1, 2, 3, 4, 5, 6\} \) under the operation of multiplication modulo 7. This is a cyclic group and a generator is, for example, the element \( \alpha = 3 \). The graph of this group is shown in the next figure.

![Graph of Example 1](image)

Example 2: Define \( G = \{1, 4, 10, 13, 16, 19\} \). These elements form a group under the operation of multiplication modulo 21. A generator for this group is the set \( \{ \alpha = 4, \beta = 13 \} \). The graph of this group is (solid lines for \( \alpha \) and dotted lines for \( \beta \))

![Graph of Example 2](image)

Example 3: Consider the following set of invertible \( 2 \times 2 \) matrices over GF(2):

\[
I = M_9 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad M_7 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad M_{14} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \\
M_6 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad M_{13} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad M_{11} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}
\]

These matrices form a group under the operation of matrix multiplication modulo 2. This group can be generated by the set \( \{ \alpha = M_7, \beta = M_6 \} \). The graph of this group is (solid lines for \( \alpha \) and dotted lines for \( \beta \))
(a) A permutation $\pi$ of $n$ can be described mathematically as

$$\pi = \begin{pmatrix} 0 & 1 & 2 & \ldots & n-1 \\ \pi(0) & \pi(1) & \pi(2) & \ldots & \pi(n-1) \end{pmatrix},$$

or, more economically, $\pi = (\pi(0), \pi(1), \pi(2), \ldots, \pi(n-1))$. Define concatenation of permutations (i.e., carrying out two concatenations in succession) as

$$\pi_i \circ \pi_j = (\pi_i(\pi_j(0)), \pi_i(\pi_j(1)), \pi_i(\pi_j(2)), \ldots, \pi_i(\pi_j(n-1))).$$

Thus, if $n = 4$ and $\pi_a = (1, 2, 0, 3)$, and $\pi_b = (1, 0, 3, 2)$, the following two permutations can be obtained using concatenation (note that this operation is not commutative):

$$\pi_a \circ \pi_b = \pi_{ab} = (2, 1, 3, 0) \quad \text{and} \quad \pi_b \circ \pi_a = \pi_{ba} = (0, 3, 1, 2).$$

Use $(\pi_a, \pi_b)$ as generator of a group under the operation of concatenation of permutations. Find, plot and label the graph of this group.

(b) Find two groups with 8 elements (e.g., by looking at the multiplicative subgroup of $\mathbb{Z}_m$ for some $m$’s) whose graphs are different geometrical figures. Plot and label the graphs of both groups.