Blockchain Technology Fall, 2023
Tutorial 2, Week 3 (Sep 26)
Due Date: Oct 14

Questions:

1. Determine whether the following groups are cyclic. If they are, give a generator of the group. **(30 points)**
   - $(Z_5, + \mod 5)$ (i.e., the set of numbers modulo 5 with addition as the group operation)
   - $(Z_8^*, \times \mod 8)$
2. Let GenGroup denote a generic, polynomial-time, group-generation algorithm that, on input 1^n, outputs a description of a cyclic G, its order q (with $|q| = n$), and a generator $g \in G$.
   - The description of a cyclic group specifies how elments of the group are represented as bit-strings. We assumes that each group element is represented by a unique bit-string.
   - There are efficient algorithms for computing the group operation in G, as well as for testing whether a given bit-string represents an element of G.

   Question: given an element $h \in G$, how to (efficiently) compute its inverse element in G. **(30 points)**
3. Given a cyclic group of order 13.
   Requirements: please specify the set and the binary operation, and further give the generator.**(40 points)**