Homework 2

1. For each equation in $\mathbb{Z}_n$ find all solutions for $x \in \mathbb{Z}_n$ (using any method).
   (a) $3x \equiv 10 \pmod{16}$
   (b) $7x \equiv 9 \pmod{18}$
   (c) $4x \equiv 5 \pmod{12}$
   (d) $2x \equiv 6 \pmod{12}$
2. Find the inverse of 17 (mod 99) in the group $(\mathbb{Z}_{99}^{\times}, \times)$ using the Euclidean algorithm. Show each of the steps.
3. Find the orders of the following elements.
   (a) $9 \pmod{51}$ in the group $(\mathbb{Z}_{51}, +)$
   (b) $3 \pmod{16}$ in the group $(\mathbb{Z}_{16}^{\times}, \times)$
   (c) $\sqrt{7}$ in the group $(\mathbb{R}, +)$
   (d) $\sqrt{7}$ in the group $(\mathbb{R}^{\times}, \times)$
4. Find the orders of the following elements in the general linear group $\mathrm{GL}_2(\mathbb{R})$.

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

5. Let G be a finite group and $a \in G$ any element.
   (a) Show that if $a^k = e$ then $\mathrm{ord}(a)$ divides k.
   (Hint: Write $k = \mathrm{ord}(a)q + r$ where $0 \leqslant r < \mathrm{ord}(a)$ is the remainder.)
   (b) Suppose G is abelian, and $b \in G$. Write $m = \mathrm{ord}(a)$, $n = \mathrm{ord}(b)$. Show that $\mathrm{ord}(ab)$ divides the least common multiple of m, n.
   (c) Consider the group $G = \{e, r, b, g, o, y\}$ from Lecture 1. Compute the orders of each element in G. Show part (b) is not true for non-abelian groups, in general.
6. Prove or disprove the following statements.
   (a) $(\mathbb{Q}^{\times}, \times)$ is a cyclic group.
   (b) $(\mathbb{Z}_4^{\times}, \times)$ is a cyclic group.
   (c) If a group has no proper non-trivial subgroups then it is cyclic.
   (Proper: not the whole group; non-trivial: not the trivial subgroup $\{e\}$.)
7. For any abelian group, show that the subset of elements of finite order is a subgroup.
8. Describe all of the subgroups of $(\mathbb{Z}_{48}, +)$.