# Abstract Algebra
## Day 13 Class Work

1. Compute the following in the additive group $\mathbb{Z}_{12}$.
   (a) $3+5$.
   (b) $9+7$.
   (c) The additive inverse of 4. ← i.e., $4+k=0$.

2. The following are to be done in the multiplicative group $U_{13}$.
   (a) Find the smallest positive integer $k$ such that $2^3 \cdot 2^5 = 2^k$.
   (b) Same as above, but with: $2^9 \cdot 2^7 = 2^k$. **Hint:** Recall that $2^{12}=1$.
   (c) Find the smallest positive integer $k$ such that $2^4 \cdot 2^k = 1$. **Ans to (c):** $k=8$.
   **Note:** In other words, $2^k$ is the multiplicative inverse of $2^4$.

3. Our friends are having the following conversation.

   **Elizabeth:** The groups $\mathbb{Z}_{12}$ and $U_{13}$ are the same. ← We'll formalize this notion of same-ness soon.

   **Anita:** Yeah, they have the same number of elements.

   **Elizabeth:** Well, their operations match up, too.

   What might Elizabeth mean? Describe as *precisely* as possible.

   **Hint:** Compare Problems #1(a) with #2(a); #1(b) with #2(b); and #1(c) with #2(c).

4. Let $g$ be an element of a multiplicative group with $\text{ord}(g)=12$.
   (a) Find the smallest positive integer $k$ such that $g^{-1}=g^k$. **Ans to (a):** $k=11$.
   (b) Same as above, but with $g^{-1}$ replaced by each of the following: $g^{-3}$, $g^{197}$, $g^{-197}$.
   (c) Is it possible that $g^8=g^5$? Why or why not? **Ans:** No. (Why not?)

5. Again, let $g$ be an element of a group $G$ with $\text{ord}(g)=12$. Define $H=\{g^k \mid k \in \mathbb{Z}\}$. ← $H$ is a subset of $G$. Do you see why?
   (a) Anita says that $H$ has infinitely many elements, since it contains all integer powers of $g$. Do you agree or disagree with her?
   (b) How many elements does $H$ actually contain? Explain your reasoning. **Ans:** 12 elements.
   (c) **Prove:** $H$ is a subgroup of $G$.

6. Recall that 2 is a generator of the multiplicative group $U_{13}$. Find all generators of $U_{13}$.

   **Hint:** What did Elizabeth say about $\mathbb{Z}_{12}$ and $U_{13}$?

7. Determine if each group below is cyclic (i.e., it has a generator):

   (a) $U_5$ (b) $U_{12}$ (c) $U_{14}$ (d) $D_4$

8. (a) Verify that 2 is a generator for $U_{19}$.
   (b) Find all generators of $U_{19}$. ← There are six of them.

9. **Prove:** Let $a \in \mathbb{Z}_m$. Then $a$ is a generator of $\mathbb{Z}_m$ if and only if $\gcd(a,m)=1$.

   **Example:** The generators of $\mathbb{Z}_{12}$ are 1, 5, 7, 11.