HOMEWORK 6

Let G be a group.

(1) Define a map $\varphi : G \to G$ by sending any $g \in G$ to g^2. Show that φ is a homomorphism of groups if and only if G is a abelian.
(2) Define a map $\varphi : G \to G$ by sending any $g \in G$ to g^{-1}. Show that φ is a homomorphism of groups if and only if G is a abelian.
(3) Show that if a homomorphism from $\mathbb{Z}$ to itself has a non-trivial kernel, then it must be the zero map.
(4) Make a table which lists every element of $\mathbb{Z}_{12}$ along with its (additive) order.
(5) In this problem we will explore the set of units (i.e. invertible elements) of $(\mathbb{Z}_n, \cdot)$.
   (a) Show that the set of elements of $\mathbb{Z}_n$ which have a multiplicative inverse (i.e. the set of elements of $x \in \mathbb{Z}_n$ so that there exists an element $y \in \mathbb{Z}_n$ so that $xy = 1$) forms an abelian group under the operation of multiplication mod n which we will denote $U(\mathbb{Z}_n)$.
   (b) Prove the following are equivalent
      (i) a mod n $\in U(\mathbb{Z}_n)$
      (ii) a is relatively prime to n
      (iii) a generates the additive group $\mathbb{Z}_n$
      (iv) a has order n in the additive group $\mathbb{Z}_n$.
   (c) Look up the Euler totient function either online or in a textbook. State its formula and its relevance to this sequence of problems.
   (d) Show that $U(\mathbb{Z}_5)$, $U(\mathbb{Z}_7)$, $U(\mathbb{Z}_{11})$ and $U(\mathbb{Z}_{13})$ are cyclic by explicitly finding an element of order equal to the order of the group. Make a conjecture about $U(\mathbb{Z}_p)$ (interestingly one needs a little bit of field theory in order to prove this conjecture).
   (e) Show that $U(\mathbb{Z}_9)$ is cyclic but $U(\mathbb{Z}_8)$ is not.
   (f) More generally show that $U(\mathbb{Z}_{2^n})$ is never cyclic for n an integer ≥ 3 (**hint** show that it has too many elements of order 2).
(6) Let G be a group and H a subgroup of G. Suppose that m is relatively prime to the order of some element $g \in G$ and that $g^m \in H$. Then show that $g \in H$.
(7) Complete (with a one word answer) and prove the following: $|a| = |a^2|$ if and only if $|a|$ is ...