MATH 534 – HOMEWORK 1

Our first problems deal with proving the things left to homework about $(\mathbb{Z}/n, +)$ and $((\mathbb{Z}/n)^\times, \cdot)$:

(1) Prove that $(a +_n b) +_n c = a +_n (b +_n c)$ for $a, b, c \in \{0, 1, \ldots, n-1\}$, thus finishing our proof from lecture that in the "numbers" definition of $\mathbb{Z}/n$, addition is associative. (Hint: we showed in lecture that the LHS equaled the remainder when $a + b + c$ is divided by n; show that the RHS equals this as well, by mimicking our proof from class).

(2) Show the following:
   (a) For $a, a', b, b' \in \mathbb{Z}$, if $a \equiv a' (\text{mod } n)$ and $b \equiv b' (\text{mod } n)$, then $ab \equiv a'b' (\text{mod } n)$.

   (b) For $a, b, c \in \{0, 1, \ldots, n-1\}$, $a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c$. (Hint: as in the case for addition, try to "meet in the middle.")

   (c) For $a, c \in \mathbb{Z}$, show that if $\gcd(a, n) = 1$ and $\gcd(c, n) = 1$, then $\gcd(ac, n) = 1$. (This shows that we have a binary operation on $((\mathbb{Z}/n)^\times, \cdot)$ in the "numbers" presentation...)

   (d) For $a, c \in \mathbb{Z}$, if $\gcd(a, n) = 1$ and $a \equiv c (\text{mod } n)$, then $\gcd(c, n) = 1$. (...and we additionally need this if we want to work in the "equivalence classes" definition!)

   Having, completed these exercises, we'll now be confident that $(\mathbb{Z}/n, +)$ and $((\mathbb{Z}/n)^\times, \cdot)$ are groups, and will stop worrying about our particular presentation of them!

   Our last two problems concern some general consequences of the axioms of a group, i.e. they can be proved assuming only that $(G, \cdot)$ consists of a set G together with a binary operation $\cdot$ that satisfies conditions I., II., and III. from lecture. If you're having trouble with them, we'll prove some similar facts on Monday, so you can see some examples of similar arguments.

(3) Let $(G, \cdot)$ be a group. For $g \in G$ and $k \in \mathbb{N}$, define $g^k = \overbrace{g \cdots g}^{k}$, *i.e.* g^k is the result of combining g with itself k times using the binary operation on the group. Prove that $(g \cdot h)^2 = g^2 \cdot h^2$ if and only if $g \cdot h = h \cdot g$.

(4) Let $(G, \cdot)$ be a group.

(a) Show that if $h \in G$ satisfies $h \cdot g = g$ for some $g \in G$, then h is the identity.

(b) Fix $k \in G$. Show that if $h \cdot k = e$, then $h = k^{-1}$.

(Note: this problem says that *if we already know that G is a group*, we can confirm that an element in G is the identity or a certain element's inverse by checking less than the definition of a group requires.)