MAT 631 — HOMEWORK 1

DUE ON TUESDAY 3 SEPTEMBER

1. Let $n \in \mathbb{Z}$ with $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a < n$. For this problem you may use the fact that if $d = \gcd(a, b)$, then there exist integers x and y such that $d = ax + by$, and d is the smallest integer with this property.

(a) If a and n are relatively prime, prove that there exists $c \in \mathbb{Z}$ with $ac = 1 (\mathrm{mod}\, n)$.

(b) If a and n are *not* relatively prime, prove that there is an integer b with $1 \leq b < n$ and $ab = 0 (\mathrm{mod}\, n)$, and conclude that there does not exist an integer c with $ac = 1 (\mathrm{mod}\, n)$.

(c) Conclude that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$.

2. Write out the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/8\mathbb{Z})^\times$ and $(\mathbb{Z}/12\mathbb{Z})^\times$. Draw a conclusion.

3. Show that if $ab = 1$ in a group G, then $b = a^{-1}$. (The point is that we don't know G is Abelian, so can't immediately conclude $ba = 1$ too.)

4. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \geq 1\}$. Prove that G is an Abelian group under multiplication, and that G is not an Abelian group under addition.

5. If x and g are elements of a group G, prove that $|x| = |g^{-1}xg|$. Conclude that $|ab| = |ba|$ for every $a, b \in G$.

6. If a and b are two commuting elements of a group G, prove that $(ab)^n = a^n b^n$ for every $n \in \mathbb{Z}$. (Do positive n first.) Give an example of non-commuting elements where this fails.