

MAT 631 — HOMEWORK 1

DUE ON TUESDAY 4 SEPTEMBER

- Let $n \in \mathbb{Z}$ with $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a < n$.
 - If a and n are relatively prime, prove that there exists $c \in \mathbb{Z}$ with $ac = 1 \pmod{n}$.
 - If a and n are *not* relatively prime, prove that there is an integer b with $ab = 0 \pmod{n}$, and conclude that there does not exist an integer c with $ac = 1 \pmod{n}$.
 - Conclude that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$.
- 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.
- Let $(G, *)$ be a group and $a_1, \dots, a_n \in G$. Prove that the n -fold product $a_1 * \dots * a_n$ is well-defined, independent of parenthesization.
- 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.)
- 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.
- If x and g are elements of a group G , prove that $|x| = |g^{-1}xg|$. Conclude that $|ab| = |ba|$ for every $a, b \in G$.
- If a and b are two 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.