Test 2 Math 301/601

Solutions

Problem 1. Let $n \in \mathbb{N}$ with $n > 1$, and let $a \in \mathbb{Z}$.

(a) Prove that if $\gcd(a, n) = 1$ and $b, c \in \mathbb{Z}$ such that $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

(b) Give an example of integers n, a, b, c such that $a \not\equiv 0 \pmod{n}$, $b \not\equiv c \pmod{n}$, and $ab \equiv ac \pmod{n}$.

Solution. (a) As $ab \equiv ac \pmod{n}$, we have that $n \mid (ab - ac)$, or equivalently, $n \mid [a(b-c)]$. Using that $\gcd(a, n) = 1$, we can apply Euclid's lemma (or rather the version proved on HW1), to conclude that $n \mid (b - c)$. Hence, $b \equiv c \pmod{n}$, as desired.

(b) Let $n = 4$, $a = 2$, $b = 1$, and $c = 3$. Then $ab = 2$ and $ac = 6$. Therefore, $ab \equiv ac \pmod{n}$ but $b \not\equiv c \pmod{n}$. □

Problem 2. Let G be a group. Prove that if $(ab)^2 = a^2b^2$ for all a and b in G, then G is abelian.

Solution. Let $a, b \in G$. We want to show that $ab = ba$. By assumption, $(ab)^2 = a^2b^2$, which we can write as $abab = aabb$. Multiplying both sides by a^{-1} on the left results in the equality $bab = abb$. Now, multiplying both sides by b^{-1} on the right results in the equality $ba = ab$, which is as desired. □