Math 453: Problem Set 2

Due at 11:00am on Wednesday, January 26, 2022

The essence of mathematics is its freedom. –Georg Cantor

(1) Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$, and suppose $\gcd(m, n) = 1$. Prove that

$$a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n} \iff a \equiv b \pmod{mn}.$$

(2) The group $U(n)$, the multiplicative group of units of $\mathbb{Z}_n$, is defined as

$$U(n) = \{a \in \mathbb{Z}_n : (\exists x \in \mathbb{Z}_n)\ ax = 1\}.$$

Prove that $U(n) = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.

(3) Let G is a group with identity e and group operation written as concatenation. Prove that, if $a^2 = e$ for all $a \in G$, then G is abelian.

(4) Define D_4 to be the symmetry group of a square, that is, the group of rotations and reflections in the plane that map a square back onto itself. (D_4 has 8 elements.) Compute and write out the Cayley table (operation table) for D_4. You will have to choose your own labelling for the elements of D_8; explain your labelling.

(5) (a) Compute and write out the Cayley table for the quaternion group Q_8, described in Example 3.15 in the textbook.

(b) Show that the group D_4 and the group Q_8 are different groups—that is, there is no relabelling and reordering of the elements of D_4 that transforms the Cayley table for D_4 into the Cayley table for Q_8. (Hint: Look for an intrinsic property that one group has, but the other doesn't.)

(6) The **order** of an element g in a group G is the smallest positive integer k such that $g^k = e$. For each odd integer n with $1 \leq n < 100$, use Sage (or another computer algebra system or programming language) to compute the order of the group element 2 in $U(n)$—that is, find the smallest positive integer k such that $2^k \equiv 1 \pmod{n}$. Organize your data in a table. Do you notice any patterns? Remark on at least one pattern that you notice.