Math 255 - Spring 2022
Advanced congruence proofs
10 points

This homework invites you to work on slightly less straightforward proofs about congruences. To do this homework, you will need the following definition: A set $\{a_1, a_2, \ldots, a_n\}$ of integers is a **complete set of residues modulo** n if every integer is congruent modulo n to one and only one of the a_is.

1. Prove that a set of n integers is a complete set of residues modulo n if and only if no two of the integers are congruent modulo n.

2. If $\{a_1, a_2, \ldots, a_n\}$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $\{aa_1, aa_2, \ldots, aa_n\}$ is also a complete set of residues modulo n.

3. Let c be any integer, and let $\gcd(a, n) = 1$. Prove that the set

$$\{c, c + a, c + 2a, c + 3a, \ldots, c + (n - 1)a\}$$

is a complete set of residues modulo n.

4. (a) Show that if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod{n}$, where $n = \text{lcm}(n_1, n_2)$.

   (b) Show that if $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, then $b \equiv c \pmod{n}$, where $n = \gcd(n_1, n_2)$.