Math 341 Exam 3

Theo Koss

November 2020

1 Problem 1

Give an example of a relation that is reflexive and transitive, but not symmetric.

Proof. Consider the set $X = \{1, 2, 3\}$ and the relation $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3), (1, 3)\}$. This is reflexive because all of $(1, 1), (2, 2), (3, 3)$ are in the relation. It is transitive because $1R2, 2R3 \implies 1R3$ is true. However it is not symmetric because $(1, 3)$ is in the relation, but $(3, 1)$ is not. In other words, you can start at 1 and get to 3, but you can't start at 3 and get to 1. QED

2 Problem 2

Fix $n \in \mathbb{N}$, prove that if $a \equiv b \mod n$, and $c \equiv d \mod n$, then $ac \equiv bd \mod n$.

Proof. By definition, if $a \equiv b \mod n$, then

$$b = a + nk$$

, for some $k \in \mathbb{Z}$ and similarly,

$$d = c + nl$$

for some $l \in \mathbb{Z}$.
N2S: $bd = ac + nq$, since this shows $bd \equiv ac \mod n$. So

$$bd = (a + nk)(c + nl) = ac + anl + cnk + n^2kl$$

Thus,

$$bd = ac + n(al + ck + nkl)$$

Let $q = (al + ck + nkl)$. This shows that $bd = ac + nq$, for some $q \in \mathbb{Z}$, therefore $bd \equiv ac \mod n$. QED

3 Problem 3

Determine if $x \mod n$ is invertible, and if yes, find its inverse for the following pairs:

1. $x = 15, n = 42$. By problem 10.1, an element $x \mod n$ is invertible iff $\gcd(x, n) = 1$. In this case, $\gcd(15, 42) = 3$, therefore x is a zero divisor, and therefore has no inverse.

2. $x = 22, n = 13$. $x \equiv 9 \mod 13$, and by the same argument, $\gcd(9, 13) = 1$, so x has an inverse, $x' = 3$, since $9 \cdot 3 = 27 \equiv 1 \mod 13$.

4 Problem 4

Let $n \in \mathbb{N}$ and $y \in \mathbb{Z}_n$. Suppose that the left multiplication map $L_y : \mathbb{Z}_n \to \mathbb{Z}_n$ is bijective. Prove that y is invertible.

Proof. N2S: $\exists y' \in \mathbb{Z}_n$ such that $y'y \equiv 1 \mod n$.
If the left multiplication map $L_y : \mathbb{Z}_n \to \mathbb{Z}_n$ is bijective, then it is injective and surjective. By the definition of surjectivity, this means every number $x \in \{1, 2, ..., n-1\}$ is mapped to. This means there must be some mapping L_y from y to 1, and therefore y has an inverse (is invertible). QED

5 Problem 5

Find $1120^{1012} \mod 11$.
Note $1120 \equiv 9 \mod 11$, and by FlT, since 11 is prime, $a^{10} \equiv 1 \mod 11$.

$$9^{1012} = 9^{10 \cdot 101 + 2} = (9^{10})^{42}(9^2) = 1 \cdot 9^2 = 81 \equiv 4 \mod 11$$