Math 341 Homework 11

Theo Koss

November 2020

1 Practice problems

1.1 Problem 11.1

Let p be prime, solve the equation $x^2 \equiv 1$ in $\mathbb{Z}_p$. (Find all solutions, and prove that there are no other solutions.)

Proof.

$$x^2 = 1 \implies x^2 - 1 = 0 \implies (x+1)(x-1) = 0$$

Assume $(x+1)$ is nonzero, because we are in $\mathbb{Z}_p$, all nonzero elements are invertible. So multiplying by $(x+1)^{-1}$:

$$(x+1)(x+1)^{-1}(x-1) = 0(x+1)^{-1} \implies (x-1) = 0, \text{ so } x = 1$$

Now assume $(x-1)$ is nonzero. Again, $(x-1)$ is invertible, so multiplying by $(x-1)^{-1}$ yields a similar result:

$$(x-1)(x-1)^{-1}(x+1) = 0(x-1)^{-1} \implies (x+1) = 0, \text{ so } x = -1$$

These are the only 2 cases for which this is true, $x = 1, -1$. QED

1.2 Problem 11.4

Let p be prime, let $S = \mathbb{Z}_p - \{0\} = \{[1]_p, [2]_p, ..., [p-1]_p\}$. Prove that for $y \neq 0$, L_y restricts to a bijective map $L_y|_S : S \to S$. (Prove that there are no 0 divisors in $\mathbb{Z}_p$)

Proof. N2S: $\nexists x \in S$, such that $L_y(x) = 0$. To the contrary, assume such an x does exist.
Suppose
$$L_y(x) = 0$$
then
$$yx = 0$$
Since $y \in S$, it is invertible, ($\exists y' \in S$ s.t. $yy' = 1$). Multiply by y' on both sides:
$$yy'x = 0y'$$
This yields: $x = 0$ $\lightning$ Because $0 \notin S$. So L_y restricts to a bijective map $S \to S$. QED

1.3 Problem 11.7

Find $2019^{2020} \mod 43$.
By FlT, (Fermat's Little Theorem) Since 43 is prime, any $a^{42} = 1 \mod 43$.

$$2020 = 42 \cdot 48 + 4, \text{ and } 2019 = -2 \mod 43$$

$$2019^{2020} = (-2^{42})^{48}(-2^4)$$

As stated above, by FlT,

$$(-2^{42})^{48} = 1^{48} = 1 \mod 43$$

So
$$(-2^{42})^{48}(-2^4) = 1 \cdot -2^4 = 16 \mod 43$$