Math 341 Homework 10

Theo Koss

October 2020

1 Practice problems

1.1 Problem 10.1

Let $a, n \in \mathbb{N}$, $n > 1$ be relatively prime. Prove that $[a]_n$ has a multiplicative inverse in Z_n.

Proof. Since gcd can be written as a linear combination, and a, n being relatively prime implies $\gcd(a, n) = 1$, then

$$ax + ny = 1$$

Is true. We can take both sides modulo n:

$$(ax + by) \mod n = 1 \mod n$$

This can be rewritten as:

$$[a]_n[x]_n + [n]_n[y]_n = [1]_n$$

Since $n \equiv 0 \mod n$,

$$[a]_n[x]_n + [n]_n[y]_n = [a]_n[x]_n + 0 \cdot [y]_n = [1]_n$$

Then, by definition,

$$[a]_n[x]_n = [1]_n$$

As required, $x \in \mathbb{Z}_n$ is the inverse of a. QED

1.2 Problem 10.3

Find all the invertible elements of $\mathbb{Z}_{10}$.

Remark. *By problem 10.1, an element $a \in \mathbb{Z}_x$ is invertible iff* $\gcd(a, x) = 1$*, that is to say that the only invertible elements are relatively prime to the modulus x.*

Therefore the invertible elements in $\mathbb{Z}_{10}$ are $\{1, 3, 7, 9\}$. We can also check that this is correct because Euler's Totient function, $\phi(10) = 4$, which is the number of elements relatively prime to 10. :)

1.3 Problem 10.4

Let p be a prime, find all invertible elements of $\mathbb{Z}_p$.
As described above, invertible elements are all of the elements $a \in \mathbb{Z}_p$ such that $\gcd(a, p) = 1$. Since p is prime, it is relatively prime to every number smaller than it, so the invertible elements of $\mathbb{Z}_p$ are: $\{1, 2, ..., p-1\}$.