LECTURE 13

The Structure of $\mathbb{Z}_p$ when p is Prime

THEOREM 13.1. *If $p > 1$ is an integer, then the following properties are equivalent.*

(1) *p is prime.*
(2) *For any $[a]_p \neq [0]_p$ in $\mathbb{Z}_p$, the equation $[a]_p X = [1]_p$ has a solution in $\mathbb{Z}_p$.*
(3) *Whenever $[a]_p[b]_p = [0]_p$ in $\mathbb{Z}_p$, then $[a]_p = [0]_p$ or $[b]_p = [0]_p$.*

Proof.

(1) $\Rightarrow$ (2) Suppose p is a positive prime and $[a]_p \neq [0]_p$ in $\mathbb{Z}_p$. We want to show that the equation $[a]_pX = [1]_p$ has a solution in $\mathbb{Z}_p$. Now since $[a]_p \neq [0]_p$,

$$a - 0 \neq kp$$

so a is not divisible by p. Since the only divisors of p are ± 1 and $\pm p$ and because $p \nmid a$, we must have

$$GCD(a, p) = 1 \quad .$$

But then by Theorem 1.3, there exists integers u and v such that

$$ua + vp = 1 \quad .$$

This equation, however, is equivalent to

$$ua - 1 = -vp$$

which implies that $ua \equiv 1 \pmod{p}$, or $[ua]_p = [1]_p$. Setting $X = [u]_p$ we have

$$[a]_p[x]_p = [a]_p[u]_p = [au]_p = [1]_p \quad ,$$

so $X = [u]_p$ is a solution.

(2) $\Rightarrow$ (3) Suppose $[a]_p[b]_p = [0]_p$ in $\mathbb{Z}_p$. If $[a]_p = [0]_p$ there is nothing to prove, If $[a]_p \neq [0]_p$ then by (2) there exists a solution $[u]_p \in \mathbb{Z}_p$ such that

$$[u]_p[a]_p = [1]_p \quad .$$

But then

$$[0]_p = [u]_p \cdot [0]_p = [u]_p\left([a]_p[b]_p\right) = \left([u]_p[a]_p\right)[b]_p = [1]_p[b]_p = [b]_p \quad .$$

Hence, in every case we have either $[a]_p = [0]_p$ or $[b]_p = [0]_p$.

(3) $\Rightarrow$ (1) Let a be any divisor of p; say $p = ab$. In order to show that p is prime we must show $a = \pm 1, \pm p$. Now

$$p = ab \quad \Rightarrow \quad ab - 0 = p \quad \Rightarrow \quad [ab]_p = [0]_p \quad \Rightarrow \quad [a]_p[b]_p = [0]_p \quad .$$

in $\mathbb{Z}_p$. By (3) then either $[a]_p = [0]_p$ or $[b]_p = [0]_p$. Now $[a]_p = [0]_p$ implies $a - 0 = kp$ which implies $p \mid a$, or that $a = sp$. But then

$$p = ab = spb.$$

Dividing both sides by p shows that $sb = 1$. Since s and b are integers the only possibilities are that $s = \pm 1$ and $b = \pm 1$. Hence $b = \pm 1$ and so $a = \pm p$. On the other hand, a similar argument shows that when $[b]_p = 0$, we must have $a = \pm 1$ and $b = \pm p$. Hence if (3) holds, then the only factors of p are ± 1 and $\pm p$, so p is prime. $\square$

We'll now prove three easy corollaries to this theorem.

COROLLARY 13.2. *Let p be a positive prime. For any $[a]_p \neq 0$ and any $[b]_p \in \mathbb{Z}_p$, the equation $[a]_p X = [b]_p$ has a unique solution in $\mathbb{Z}_p$.*

Proof. We need to prove that two things, that $[a]_p X = [b]_p$ has a solution in $\mathbb{Z}_p$ and that that solution is unique.

Existence: Since p is prime, by (2) of the preceding theorem, $[a]_p X = [1]_p$ has a solution in $\mathbb{Z}_p$. Let $[c]_p$ be that solution. Multiplying both sides of this equation by $[b]_p$, we get

$$[b]_p [a]_p [c]_p = [b]_p [1]_p \quad \Longrightarrow \quad [a]_p \left([bc]_p\right) = [b]_p$$

Thus, $[bc]_p$ will be a solution of $[a]_p x = [b]_p$.

Uniqueness: Suppose both

$$\begin{aligned} [a]_p [c_1]_p &= [b]_p \\ [a]_p [c_2]_p &= [b]_p \end{aligned}$$

Subtracting these two equations we have

$$[a_p] \left([c_1]_p - [c_2]_p\right) = [0]_p$$

Since p is prime and $[a]_p \neq [0]_p$ by hypothesis, statement (3) of the preceding theorems says

$$[c_1]_p - [c_2]_p = [0]_p \quad \Longrightarrow \quad [c_1]_p = [c_2]_p \quad .$$

□

COROLLARY 13.3. *Let a and n be integers with $n > 1$. Then $GCD(a, n) = 1$ if and only if the equation $[a]_n X = [1]_n$ in $\mathbb{Z}_n$ has a solution.*

Proof.

$\Rightarrow$

Suppose $GCD(a, n) = 1$. Then by Theorem 1.3, there exist integers u and v such that

$$1 = au + nv \quad .$$

But then

$$au - 1 = nv$$

so au is congruent to 1 modulo n. Hence

$$[1]_n = [au]_n = [a]_n [u]_n \quad .$$

Thus, $[u]_n$ is a solution of $[a]_n X = [1]_n$ in $\mathbb{Z}_n$.

$\Leftarrow$

Suppose $[a]_n [x]_n = [1]_n$ has a solution $[u]_n$ in $\mathbb{Z}_n$. Then au is congruent to n modulo n. But this implies

$$au - 1 = nq$$

or

$$au - nq = 1 \quad .$$

It follows from this equation that any common divisor of a and n must divide 1. Therefore, $GCD(a, n) = 1$. □

DEFINITION 13.4. *Whenever there is solution in $\mathbb{Z}_n$ to the equation $[a]_n X = [1]_n$ we say that $[a]_n$ is a **unit** in $\mathbb{Z}_n$. Whenever there is a non-trivial solution (i.e, a solution other than the obvious one $X = [0]_n$) of $[a]_n X = [0]_n$ we say that $[a]_n$ is a **zero divisor** in $\mathbb{Z}_n$.*

LEMMA 13.5. *Let n be a positive integer. If $[a]_n \in \mathbb{Z}_n$, then $[a]_n$ is either a unit or a zero divisor.*

Proof. From the fact that $GCD\,(a,n) \geq 1$ always, we have two distinct cases:

- $GCD\,(a,n) = 1$. In this case, we know from Corollary 13.3 that $[a]_n$ is a unit in $\mathbb{Z}_n$. We will show that $[a]_n$ cannot also be a zero divisor. Suppose we had an element $[b]_n \neq [0]_n$ such that $[a]_n [b]_n = [0]_n$. Let $[a]_n^{-1}$ be the solution of $[a]_n X = [1]_n$ guaranteed by Corollary 13.3.Then we would have
$$\begin{aligned} [1]_n &= [a]_n [a]_n^{-1} \\ &\Rightarrow \quad [b]_n [1]_n = [b_n]_n \left([a]_n [a]_n^{-1}\right) \\ &\Rightarrow \quad [b]_n = ([b]_n [a]_n) [a]_n^{-1} = [0]_n [a]_n^{-1} = [0]_n \end{aligned}$$
which contradicts our hypothesis that $[b]_n \neq [0]_n$. Therefore when $GCD\,(a,n) = 1$, $[a]_n$ is a unit but **not** a zero divisor.
- Suppose $GCD\,(a,n) = d > 1$. In this case, the "if and only if" part of Corollary 13.3 tells us that $[a]_n$ can not be a unit in $\mathbb{Z}_n$. To see that $[a]_n$ is a zero divisor, we note $GCD\,(a,n) = d$ means d divides both a and n, and moreover, $1 < d \leq n$. Now if $d = n$, then this means that n divides a and so $[a]_n = [0]_n$, and hence $[a]_n$ will be a zero divisor (as any $[k]_n$ time $[0]_n$ produces $[0]_n$).
  So now we suppose $1 < d < n$. Write
$$\begin{aligned} a &= qd \\ n &= sd \quad \text{with } 1 < s,d < n \end{aligned}$$
  We then have
$$[a]_n [s]_n = [as]_n = [(qd)\,s]_n = [q\,(ds)]_n = [qn]_n = [0]_n$$
  Since $1 < s < n$ we have $[s]_n \neq [0]_n$ and yet
$$[a]_n [s]_n = [0]_n$$
  Thus, when $GCD(a,n) > 1$ $[a]_n$ is a zero divisor but **not** a unit. □

COROLLARY 13.6. *Let a, b, n be integers with $n > 1$ and $GCD\,(a,n) = 1$. Then the equation*
$$[a]_n x = [b]_n$$
has a unique solution in $\mathbb{Z}_n$.

Proof. Suppose $GCD\,(a,n) = 1$, then as above we have integers $u, v \in \mathbb{Z}$ such that
$$\begin{aligned} au + nv \quad = \quad 1 \quad &\Longrightarrow \quad [au - nv]_n = [1]_n \\ &\Longrightarrow \quad [au]_n - [nv]_n = [1]_n \\ &\Longrightarrow \quad [au]_n - [0]_n = [1]_n \\ &\Longrightarrow \quad [a]_n [u]_n = [1]_n \end{aligned}$$
Now multiply both sides by $[b]_n$ and we get
$$[a]_n ([b]_n [u]_n) = [1]_n [b]_n = [b]_n$$
So $[bu]_n = [b]_n [u]_n$ is a solution of $[a]_n x = [b]_n$.

To see that this solution is unique argue as in Corollary 13.2. Suppose we had two solutions
$$\begin{aligned} [a]_n [c_1]_n &= [b]_n \\ [a]_n [c_2]_n &= [b]_n \end{aligned}$$
Subtracting one equation from the other we get
$$[a]_n ([c_1]_n - [c_2]_n) = [0]_n \quad .$$

Because $[a_n]_n$ has no zero divisors (by Corollary 13.3 and Lemma 13.5), we must conclude that

$$[c_1]_n - [c_2]_n = [0]_n \quad \Rightarrow \quad [c_1]_n = [c_2]_n$$

and so the two solutions in fact must coincide. □

THEOREM 13.7. *Let a, b, n be integers with $n > 1$, and let $d = GCD\,(a, n)$. Then*

(i) *The equation $[a]_n\, x = [b]_n$ has a solution in $\mathbb{Z}_n$ if and only if $d|b$.*
(ii) *If $d|b$, then the equation $[a]_n\, x = [b]_n$ has d distinct solutions in $\mathbb{Z}_p$.*

Proof.

(i) $\Longrightarrow$

Suppose $[a]_n\, x = [b]_n$ has a solution in $\mathbb{Z}_n$ and let $[c]_n$ be that solution. We have

$$[a]_n\,[c]_n = [b]_n \quad \Longrightarrow \quad [ac]_n = [b]_n \quad \Longrightarrow \quad ac = b \pmod n \quad \Longrightarrow \quad ac - b = kn \quad \text{for some } k \in \mathbb{Z}$$

But then

$$(*) \qquad b = ac - kn$$

So anything that divides both a and n, will divide the right hand side of (*) and hence, b (the left hand side of (*)). In particular, the greatest common divisor of a and n divides the right hand side of (*), so $d = GCD(a, n)$ divides b.

(i) $\Longleftarrow$

Suppose $d = GCD(a, n)$ and $d|b$. Since $d = GCD\,(a, n)$ there exists integers u, v such that

$$(**) \qquad d = au + nv$$

Since $d|b$, there exists an integer k such that $b = kd$. Now multiply both sides of (**) by k. Then we have

$$b = kd = a\,(ku) + n\,(kv) \quad \Longrightarrow \quad b \equiv a\,(ku) \pmod n \quad \Longrightarrow \quad [b]_n = [aku]_n = [a]_n\,[ku]_n$$

Hence $[ku]_n$ is a solution of $[a]_n\, x = [b]_n$.

(ii) Suppose $d = GCD\,(a, n)$ and $d|b$. In fact, since $d = GCD\,(a, n)$, $d|a$ and $d|n$. Write

$$\begin{aligned} n &= rd \\ a &= sd \end{aligned}$$

I claim $n|\,(ar)$. Indeed,

$$ar = (sd)\,r = s\,(rd) = sn \quad \Longrightarrow \quad n|\,(ar)$$

Now suppose $[c]_n$ is a solution of $[a]_n\, x = [b]_n$. I claim $[c + r]_n$ is also a solution. Indeed, if

$$[a]_n\,[c]_n = [b]_n$$

then if we replace c by $c + r$, we get

$$\begin{aligned} [a]_n\,[c + r]_n &= [a]_n\,[c]_n + [ar]_n \\ &= [b]_n + [ar]_n \qquad , \quad \text{since } [c]_n \text{ is a solution of } [a]_n\, x = [b]_n \\ &= [b]_n + [0]_n \qquad , \quad \text{since } ar \text{ is divisible by } n \\ &= [b]_n \end{aligned}$$

But if $[c + r]_n$ is a solution so is $[c + r + r]_n = [c + 2r]$, as well as $[c + 3r]_n$, etc. Clearly we can generate lots of solutions this way. The question is, when do stop getting new solutions this way (recall that $\mathbb{Z}_n$ only has n elements, so we can't get an infinite number of solutions). Well, we will keep getting new congruence classes until $[c+kr]_n = [c+n]_n$. In other words until $kr = n$. But r was defined as the solution of $dr = n$. Therefore, we'll get the following congruence classes as solutions

$$[c]_n\,, [c+r]_n\,, [c+2r]_n\,, \ldots, [c+(d-1)\,r]_n$$

It is easy to see that these are all distinct since $0 \leq kr < n$ for $k \in \{0, 1, \ldots, d-1\}$