453 **Lecture 10**

1. Cyclic groups

Finite cyclic groups

$Z_n = \{ [0], [1], \ldots, [n-1] \}$

and $[i] + [j] = [i+j]$

Here $[i]$ is the congruence class of i mod n

i.e. the equivalence class of i for the equivalence relation

$$a \sim b \text{ iff } n \mid a-b.$$

We call Z_n to be "the finite cyclic group of order n".

Infinite cyclic group is "the same as" $\mathbb{Z}$.

2. Multiplicative group of units.

$Z_n^* = \{ [i] \mid \gcd(i,n) = 1 \}$.

and the group operation is

$$[i] \cdot [j] = [ij].$$

Prop. (1) If $[i], [j] \in \mathbb{Z}_n^*$, then $[ij] \in \mathbb{Z}_n^*$.

(2) If $[i] \in \mathbb{Z}_n^*$, then there exists $[j] \in \mathbb{Z}_n^*$ such that $[ij] = [1]$.

Pf: (1) We use Bezout identity.

Since $\gcd(i, n) = \gcd(j, n) = 1$ there exists $x, y, x', y' \in \mathbb{Z}$ such that

$$1 = ix + ny$$

$$1 = jx' + ny'$$

Multiplying the two equations we get

$$1 = ij(xx') + n(ixy' + jx'y + nyy')$$

This proves that $\gcd(ij, n) = 1 \Rightarrow [ij] \in \mathbb{Z}_n^*$.

(2) Since $\gcd(i, n) = 1$, again using Bezout identity

$$1 = ix + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Now take $j = x$. The above equation shows that $\gcd(n, x) = 1 \Rightarrow [x] = [j] \in \mathbb{Z}_n^*$ and also that $[i][j] = 1$.

$\boxtimes$