LECTURE 7

(Friday OCT. 11, 2019)

<u>Reformulation</u>: Observe that when $d \mid N$ there's a natural function

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_d \qquad \sim \text{"respects" addition \& multiplication.}$$
$$[x]_N \longmapsto [x]_d$$

(why well-defined? Must check $x \equiv x' \pmod N$ $\Longrightarrow$ $x \equiv x' \pmod d$. Obvious since we're <u>assuming</u> $d \mid N$)

<u>Thm</u> (CRT — version II): Suppose $GCD(M,N) = 1$. The natural map

$$f: \mathbb{Z}_{MN} \longrightarrow \mathbb{Z}_M \times \mathbb{Z}_N \quad \text{(:group under vector addition)}$$
$$[x]_{MN} \longmapsto ([x]_M, [x]_N)$$

is a <u>bijection</u>, which preserves $+$ and $\cdot$.

("isomorphism")

<u>PROOF</u>: f is <u>injective</u>: $f([x]_{MN}) = f([y]_{MN})$ means $[x]_M = [y]_M$ <u>and</u> $[x]_N = [y]_N$. In other words $x \equiv y \ (M)$ and $x \equiv y \ (N)$. So $x - y$ is a common multiple of M, N — equivalently a multiple

M,N coprime.

of $LCM(M,N) = MN$. Translates into $x \equiv y \ (MN)$.

— conclude $[x]_{MN} = [y]_{MN}$ which is injectivity.

Now, f is automatically surjective since

$$|\mathbb{Z}_{MN}| = MN = |\mathbb{Z}_M \times \mathbb{Z}_N|. \quad \square$$

(really an altenative proof of CRT..)

$\Longrightarrow$ Multiplicative Analogue: the restriction

$$f: \mathbb{Z}_{MN}^{\times} \longrightarrow \mathbb{Z}_M^{\times} \times \mathbb{Z}_N^{\times}$$

is bijective (and preserves $\bullet$). — still assuming $GCD(M,N) = 1$.

Corollary φ is a multiplicative function, i.e.:

$$\varphi(MN) = \varphi(M)\varphi(N) \quad \text{provided } M,N \text{ coprime}.$$

— allows us to compute φ from the prime factorization of N.

p^n-Formula: $\quad \varphi(p^n) = p^n - p^{n-1} \quad \forall n \geq 1.$
(p = prime)

<u>Why?</u> Count positive $a < p^n$ coprime to p^n

– How many p-multiples $< p^n$?

since p = prime this amounts to $p \nmid a$.

$0p, 1p, 2p, 3p, \ldots, mp,$

where $m = p^{n-1} - 1$. ✓

<u>Ex</u>: Calculate $\varphi(2^3 \cdot 3^2 \cdot 5^4) =$

$$\varphi(2^3)\varphi(3^2)\varphi(5^4) = (2^3 - 2^2)(3^2 - 3)(5^4 - 5^3)$$
$$= 4 \cdot 6 \cdot 500 = 12000.$$

<u>Remark</u>: M, N must be coprime in CRT.

Ex.) the natural map

$$f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$[x]_4 \longmapsto ([x]_2, [x]_2)$$

is <u>not</u> injective: $f([2]) = ([0],[0]) = f([0])$

<u>but</u> $[2]_4 \neq [0]_4$.

– The two groups are "non-isomorphic":

$\mathbb{Z}_4$ <u>cyclic</u>, $\mathbb{Z}_2 \times \mathbb{Z}_2$ non-cyclic

(compare w. $\mathbb{Z}_{10}^\times$ and $\mathbb{Z}_{12}^\times$ resp.)

KLEIN'S 4-GROUP.