# Lecture 2

**Lemma**: Let $z^d \equiv 1 \mod n$. Then $e(z) \mid d$

**Proof**: By Euclid let

$$d = q\,e(z) + r, \quad 0 \le r < e(z)$$

Then

$$z^d = z^{q e(z) + r}$$

$$= \big(\underbrace{z^{e(z)}}_{\equiv 1 \bmod n}\big)^q \cdot z^r$$

$$\equiv 1 \cdot z^r \mod n$$

But $z^d \equiv 1 \mod n \Rightarrow z^r \equiv 1 \mod n$ contradicts minimality of $e(z)$. Thus $r = 0 \Rightarrow e(z) \mid d$.

**Exercise**: Check that if $\exists\, e$ s.t.

$$z^e \equiv 1 \mod n \quad \text{then } GCD(n, z) = 1.$$

In other words, there is no way to define order of an element outside of $\mathbb{Z}/n\mathbb{Z}^\times$.

Corollary : $\forall z \in \mathbb{Z}/n\mathbb{Z}^\times$
$e(z) \mid \varphi(n)$.

Primitive roots

Let $p$ be a prime. We call $z$ to be a primitive root mod $p$ if we have $e(z) = \varphi(p) = p-1$.

Ex.: Let $p = 7$

a) 3 is a primitive root mod 7

as $3^6 = 9^3 \equiv 2^3 \bmod 7$
$= 8 \equiv 1 \bmod 7$.

However, $3^1, 3^2, 3^3 \not\equiv 1 \bmod 7$

b) 2 is NOT a primitive root mod. 7.

Of course $2^6 = 8^2 \equiv 1 \bmod 7$

But also $2^3 = 8 \equiv 1 \bmod 7$

i.e. $e(2) \neq 6$.

How to find the numbers of elements in $\{1, \ldots, p-1\}$ whose order is $d$.
$\uparrow$ prime
(if at all exists)

<u>Theorem</u>: Let $p$ be a prime and $d \mid p-1$. Then the number of elements of order $d$ in $\{1, \ldots, p-1\}$ is $\varphi(d)$.

<u>RMK</u> 1) In particular, $\forall d \mid p-1$ we may find $a \in \mathbb{Z}/p\mathbb{Z}^{\times}$ such that $e(a) = d$.

2) On the other hand, if $d$ is the order of an element in $\mathbb{Z}/p\mathbb{Z}^{\times}$ then $d \mid p-1$.

<u>Proof</u>: We first show that if $\exists$ an element $z$ with $e(z) = d$ then there are $\varphi(d)$ many such element

<u>Step 1</u>: The members $\{1, z, \ldots, z^{d-1}\}$ are all distinct mod $p$.

Indeed, if for $i \neq j$ we have

$$z^i \equiv z^j \mod p$$

$$\Rightarrow \quad z^{|i-j|} \equiv 1 \mod p$$

But $0 < |i-j| < d$ which contradicts minimality of $d$.

<u>Step 2</u> $\{1, z, \ldots, z^{d-1}\}$ all have order $\leq d$ mod $p$.

Indeed, $(z^j)^d = (z^d)^j \equiv 1 \mod p$.

$$\Rightarrow \quad d \geq e(z^j)$$

<u>Step 3</u> For $0 \leq j \leq d-1$, $z^j$ has order $d \Longleftrightarrow GCD(j, d) = 1$

"$\Longrightarrow$" If $g := GCD(j, d) > 1$ then $\frac{d}{g} < d$

But $z^{j d/g} = z^{d(j/g)} \equiv 1 \mod p$

$\in \mathbb{N}$

Thus $e(z^j) \leq \frac{d}{g} < d$

" $\Leftarrow$ " Let $e(z^j) =: r$

Then $(z^j)^r \equiv 1 \mod p$

$\Rightarrow$ $d \mid jr$ as $d = e(z)$

But $GCD(d, j) = 1 \Rightarrow d \mid r$

But in step 2 we showed $r \leq d$

$\Rightarrow$ $r = d = e(z^j)$

All in all we obtain that

$$\#\{1 \leq j \leq d-1 : e(z^j) = d\}$$

$$= \#\{1 \leq j \leq d-1 : GCD(j, d) = 1\}$$

$$= \varphi(d)$$

<u>RMK</u> i) The proof also shows if we one element $z$ of order $d$ then how to find all the others ones. They are precisely

$$\{z^j \mid 1 \leq j \leq d-1,\ GCD(j,d) = 1\}$$

2) So far we assumed there indeed exists one element with order $d$. Next exercise proves that is the case.

<u>Exercise</u>: Prove that $\sum_{d \mid n} \varphi(d) = n$

<u>Proof of existence of element with order $d \mid p-1$</u>

$\{1, 2, \ldots, p-1\}$ can be written as disjoint union of the sets

$$\bigcup_{d \mid p-1} \underbrace{\{ 1 \leq z \leq p-1 \mid z \text{ has order } d \bmod p\}}_{=: S_d}.$$

Thus $\sum_{d \mid p-1} |S_d| = p-1$

Previously, we saw that $|S_d| = 0$ or $\varphi(d)$

$$\Rightarrow \underset{\underset{p-1}{\shortparallel}}{\sum_{d \mid p-1} |S_d|} \leq \sum_{d \mid p-1} \varphi(d) = p-1$$

$$\Rightarrow \quad |S_d| = \varphi(d)$$

Exercise: Let $z$ be a primitive root mod $p$ (prime). Then show that $e(z^n) = \dfrac{p-1}{GCD(n, p-1)}$.

Exercise: Find all $z \in \mathbb{Z}/17\mathbb{Z}^{\times}$ with $e(z) = 4$.

Exercise: Convince yourself that for any function $f: \mathbb{Z} \to \mathbb{R}$

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right).$$

Exercise: Let $n \in \mathbb{N}$ & $k \in \mathbb{N}$. Prove that $\varphi(n^k) = n^{k-1}\varphi(n)$.

Compare with the statement when $n$ = prime, from Morning lecture.