Section 9.6 I

- If $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $a^{\varphi(m)} \equiv 1 \bmod m$
- Every $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ has a least positive x for which $a^x \equiv 1 \bmod m$

  $x = \operatorname{ord}_m(a)$
- $\operatorname{ord}_m(a) \mid \varphi(m)$
- Sometimes, $\operatorname{ord}_m(a) = \varphi(m)$
  - ↳ in this case $\varphi(m)$ is the best possible exponent in Euler's Thm
- What about when there is no primitive root? Is $\varphi(m)$ still the best exponent?

$m = 8$ has no primitive root

x	1	2	3	$4 = \varphi(8)$
1^x	1	1	1	1
3^x	3	1	3	1
5^x	5	1	5	1
7^x	7	1	7	1

It's true: $a^{\varphi(8)} \equiv 1 \mod 8$

Better exponent exists: $a^2 \equiv 1 \mod 8$

Def: Let $m \in \mathbb{Z}_{>0}$. A <u>universal exponent</u> for m is a $U \in \mathbb{Z}_{>0}$ s.t. $a^U \equiv 1 \mod m$ for all $a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$

Ex: $\varphi(m)$ is a universal exponent for m.

Ex: $m = 600 = 2^3 \cdot 3 \cdot 5^2$

Check $\varphi(600) = 160$

$a^{160} \equiv 1 \mod 600$ for $a \in (\mathbb{Z}/600\mathbb{Z})^\times$

Note

$a^{\varphi(8)\,2} \equiv 1 \mod 8$

$a^2 \equiv 1 \mod 3$

$a^{\varphi(25)} \equiv 1 \mod 25$

Observe that

$a^u \equiv 1 \mod 8$

$a^u \equiv 1 \mod 3$

$a^u \equiv 1 \mod 25$

$\Rightarrow a^u \equiv 1 \mod 600$

if 4 is a multiple of

$\varphi(8)^2$, $\varphi(3)$, $\varphi(25)$

Certainly $\varphi(8)^2 \varphi(3) \varphi(25) = 160$ is a multiple

So is $\operatorname{lcm}(\varphi(8)^2, \varphi(3), \varphi(25))$

$= \operatorname{lcm}(4^2, 2, 20)$

$= 20$

So $a^{20} \equiv 1 \pmod{600}$

$\forall\, a \in (\mathbb{Z}/600\mathbb{Z})^\times$

Goal: Compute minimal universal exponent, denote $\lambda(n)$

Thm: if $n > 1$, $n = 2^{e_0} \cdot p_1^{e_1} \cdots p_g^{e_g}$

for $e_0 \geq 0$, $p_1, \ldots, p_g$ distinct odd primes, $e_1, \ldots, e_g \geq 1$, then

$$\lambda(n) = \operatorname{lcm}\left(\lambda\left(2^{e_0}\right), \varphi\left(p_1^{e_1}\right), \ldots, \varphi\left(p_g^{e_g}\right)\right)$$

and $\lambda\left(2^{e_0}\right) = 2^{e_0 - 2}$ if $e_0 \geq 3$

Ex: $n = 180 = 2^2 \cdot 3^2 \cdot 5$

$\lambda(2^2) = 2$
$\varphi(3^2) = 6$ $\longrightarrow$ $\lambda(180) = \operatorname{lcm}(2, 6, 4)$
$\varphi(5) = 4$ $= 12$

Probably true: if $(m, n) = 1$, $\lambda(mn) = \operatorname{lcm}(\lambda(m), \lambda(n))$