Section 9.3

From 9.2: For any prime p, there exists a primitive root mod p.

Thm: There is a primitive root modulo n if and only if n meets one of the following criteria:

1. $n = 2$
2. $n = 4$
3. $n = p^t$ for an odd prime p and $t \geq 1$
4. $n = 2p^t$ for " .... "

Q How do we get there?

First: prove that there is a prim. rt. mod p^2

↳ if r is a prim. rt mod p, then all but one $a \in \mathbb{Z}/p^2\mathbb{Z}$ with $a \equiv r \bmod p$ is a prim. rt. mod p^2.

Ex: $p = 5$

↳ 2 is prim. rt. mod 5

$p^2 = 25$

Find all $a \in \mathbb{Z}/25\mathbb{Z}$ s.t.

$a \equiv 2 \mod 5$

E.g. $\underbrace{a = 2, 7, 12, 17, 22}_{\text{all but one is a prim. rt. mod } 25.}$

Cor: If r is a prim. rt. mod p, then r or $r+p$ is a prim. rt. mod p^2

Thm: If r is a prim. rt. mod p^2, then r is a prim. rt mod p^k for $k \geq 2$.

Thm: If r is a prim. rt. mod p^t and r is odd, then r is a prim. rt. mod $2p^t$. If r is even, then $r+p^t$ is a prim. rt. mod $2p^t$.

Recall: If $(a,n)>1$, then $\nexists x$.

$$a^x \equiv 1 \mod n$$

Next: If n does not fit one of the 4 categories, there is no primitive root mod n.

Start w/ powers of 2:

for any $r \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ where $k \geq 3$, then

$$\text{ord}_{2^k}(r) \mid \frac{\varphi(2^k)}{2}$$

Check the rest...

Algorithm for finding prim. rt. mod n:

1. Check to see if n has right form
2. $n = 2, 4$ ✓
3. $n = 2p^t$ or $n = p^t$
   a) find prim. rt. mod p (see wk 6 gp. wk)

   b) "lift" to a prim. rt. mod p^2
      - use r or $r+p$

      - get that this is a prim. rt mod p^t for free

4. If $n = 2p^t$
   - if odd, done ✓
   - if even, $r + p^t$ ✓

Ex: $n = 2 \cdot 17^5$

① $p = 17$ – find prim. rt. mod 17.

↳ 3 is a prim. rt. mod 17

– check $\left.\begin{matrix} 3^1 \\ 3^2 \\ 3^4 \\ 3^8 \end{matrix}\right\} \not\equiv 1 \mod 17$

② Is 3 a prim. rt. mod 17^2?

↳ possible orders of 3: divisors of $\varphi(17^2) = 17 \cdot 16$,

$\underbrace{1, 2, 4, 8,}_{\text{prev. step}}\ \underbrace{16, 17, 2 \cdot 17, 4 \cdot 17, 8 \cdot 17}_{\text{check 3 to these powers } \not\equiv 1 \mod 17^2},\ 16 \cdot 17$

So 3 is a prim. rt. mod $17^2 \rightarrow$ 3 is a prim rt mod 17^5

(3) Is 3 even or odd?

So 3 is a prim. rt. mod $2 \cdot 17^5$