Section 9.4

- see "intro to discrete logs"

Def. Let r be a primitive root mod m.
(Previously: $\{r, r^2, r^3, \ldots, r^{\varphi(m)}\}$ is a reduced residue system mod m)

Define the index base r (or discrete log) of a modulo m to be the smallest

$x \in \mathbb{Z}/\varphi(m)\mathbb{Z}$ s.t. $r^x \equiv a \mod m$

This is denoted $\text{ind}_r(a)$

Thm: If $m \in \mathbb{Z}_{>0}$, r is a prim. rt. mod m and $a, b \in (\mathbb{Z}/m\mathbb{Z})^\times$

Then:

1. $\text{ind}_r(1) \equiv 0 \mod \varphi(m)$
2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \mod \varphi(m)$
3. $\text{ind}_r(a^k) \equiv k \cdot \text{ind}_r(a) \mod \varphi(m)$

Aside: $\log_b(a) = \dfrac{\log a}{\log b}$

Ex: Find solns. to $\cancel{7}^{\,5} x^3 \equiv 4 \mod 9$

Note: 2 is prim. rt mod 9

?

So $\mathrm{ind}_2(\cancel{7}^{\,5} x^3) \equiv \mathrm{ind}_2(4) \mod 6$

So $\mathrm{ind}_2(\cancel{7}^{\,5}) + 3\,\mathrm{ind}_2(x) \equiv 2 \mod 6$

$5 + 3\,\mathrm{ind}_2(x) \equiv 2 \mod 6$

$3\,\mathrm{ind}_2(x) \equiv -3 \equiv 3 \mod 6$

$\rightarrow \quad \mathrm{ind}_2(x) \equiv 1 \mod \dfrac{6}{(6,3)} = 2$

$\mathrm{ind}_2(x)$ odd, mod 6

$\mathrm{ind}_2(x) \equiv 1, 3. 5 \mod 6$

$x \equiv 2^1, 2^3, 2^5 \mod 9$

Check to see if $2, 8, 2^5$ are solns.

Q: When can we solve

$$x^k \equiv a \mod m?$$

$k=2$: quadratic residues

Def: let $m, k \in \mathbb{Z}_{>0}$, $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. a is a k^{th} <u>power residue</u> mod m if there exists $x \in \mathbb{Z}$ s.t.

$$x^k \equiv a \mod m$$

In quadratic case:

Euler's Criterion stated that

a is a Q R. mod p
iff $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

Thm: Let $m \in \mathbb{Z}_{>0}$ with a primitive root. If $k \in \mathbb{Z}_{>0}$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then a is a kth power residue mod m if and only if

$$a^{\frac{\varphi(m)}{(k, \varphi(m))}} \equiv 1 \mod m.$$

Note: m odd prime, $k = 2$

$$\rightarrow a^{\frac{m-1}{(2, m-1)}} \equiv 1 \mod m$$

$$a^{\frac{m-1}{2}} \equiv 1 \mod m$$

Pf: Let r be a prim. rt. mod m

$X^k \equiv a \mod m$ has soln.

iff $\quad k \cdot \operatorname{ind}_r(x) \equiv \operatorname{ind}_r(a) \mod \varphi(m)$

has a soln. for $\operatorname{ind}_r(x)$.

iff $\quad (k, \varphi(m)) \mid \operatorname{ind}_r(a)$

iff $$\frac{\varphi(m)}{(k, \varphi(m))} \cdot \operatorname{ind}_r(a) \equiv 0 \mod \varphi(m)$$

iff $$r^{\frac{\varphi(m)}{(k,\varphi(m))} \cdot \operatorname{ind}_r(a)} \equiv 1 \mod m$$

$$\rotatebox{90}{$\equiv$}$$

$$a^{\frac{\varphi(m)}{(k, \varphi(m))}}$$

$$e^{5\log(2)} = 2^5$$

Ex: Is 5 a sixth power res. mod 17?

A: Compute $5^{\frac{\varphi(17)}{(6,\varphi(17))}}$ mod 17

$$= 5^{\frac{16}{(6,16)}} = 5^8$$

$5^2 \equiv 8 \mod 17$

$5^4 \equiv 64 \equiv 13 \mod 17$

$5^8 \equiv 169 \equiv 16 \mod 17$

$\not\equiv 1 \mod 17$

So 5 is not a sixth power residue mod 17.