1 is a primitive root for 2: $1^1 \equiv 1 \pmod 2$

3 is a primitive root for 4: $3^2 \equiv 1 \pmod 4$, $3 \not\equiv 1 \pmod 4$

8 does <u>not</u> have a primitive root: $1 \equiv 1$, $3^2 \equiv 1$, $5^2 \equiv 1$, $7^2 \equiv 1$

so $\{1, 3, 5, 7\}$ all have order 2, but

$\varphi(8) = 8 - 4 = 4$.

in general: if a is <u>odd</u>, then $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ for $k \geq 3$.

$\Longrightarrow$ 2^k does <u>not</u> have a primitive root for $k \geq 3$.

---

if $\gcd(m,n) = 1$, then mn has no primitive root.

$\hookrightarrow m, n > 2$

Lemma If p is an odd prime, then p has a primitive root r such that

$$r^{p-1} \not\equiv 1 \pmod{p^2}.$$

Pf. Let r be a primitive root of p: $r^{p-1} \equiv 1 \pmod{p}$.

If $r^{p-1} \not\equiv 1 \pmod{p^2}$, done.

If $r^{p-1} \equiv 1 \pmod{p^2}$, consider the primitive root $r+p$. [Note: $(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \dots \equiv r^{p-1} \overset{\text{mod } p}{\equiv} 1$]

Then $$(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \underbrace{\dots}_{\equiv 0 \pmod{p^2}} \equiv r^{p-1} - pr^{p-2}$$

$$\Rightarrow (r+p)^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2} \not\equiv 1.$$

$p \nmid r \Rightarrow -pr^{p-2} \not\equiv 0 \pmod{p^2}$

$\boxtimes$

<u>Corollary</u> p is an odd prime $\Longrightarrow$ p^2 has a primitive root.

<u>pf.</u> Let r be a primitive root of p s.t. $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Let n be the order of r mod p^2.

Euler $\Longrightarrow$ $r^{\varphi(p^2)} \equiv 1 \pmod{p^2} \Longrightarrow r^{p(p-1)} \equiv 1 \pmod{p^2}$.

$r^n \equiv 1 \pmod{p^2} \Longrightarrow n \mid p(p-1)$.

$\Longrightarrow r^n \equiv 1 \pmod{p} \Longrightarrow p-1 \mid n$

$\left.\right\}$ $\cancel{n = p-1}$ or $\boxed{n = p(p-1)}$ $\underline{\underline{n = \varphi(p^2)}}$

∎

Lemma p is an odd prime, r is a primitive root such that $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Then $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for $k \geq 2$.

pf. via induction. base case: previous lemma/ hypothesis

Suppose that $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for some $k \geq 2$. (IH)

Euler: $r^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}} \Longleftrightarrow r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$

$\Longrightarrow r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$ for some a, $p \nmid a$.

$\Longrightarrow \left(r^{p^{k-2}(p-1)}\right)^p = (1+ap^{k-1})^p$

$\Longrightarrow r^{p^{k-1}(p-1)} = 1 + p \cdot ap^{k-1} + \underbrace{\cdots}_{\equiv 0 \pmod{p^{k+1}}} \equiv 1 + ap^k \pmod{p^{k+1}} \not\equiv 1.$

Corollary p is an odd prime, then p^k has a primitive root (for any $k \geq 1$).

Pf. Let r be a primitive root of p s.t. $r^{p-1} \not\equiv 1 \pmod{p^2}$, so that $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for any $k \geq 2$.

Let n be the order of r mod p^k, so that

$$r^n \equiv 1 \pmod{p^k}. \implies n \mid \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

$$\implies r^n \equiv 1 \pmod{p} \implies \varphi(p) = p-1 \mid n$$

Thus: $n = p^m(p-1)$, $m \leq k-1$. $\implies m = k-1$, $n = \varphi(p^k)$.

$\boxtimes$

<u>Corollary</u> $2p^k$ has a primitive root for any $k \geq 1$.

<u>pf.</u> Let r be a primitive root of p^k. Let n be the order of r mod $2p^k$.

$$\underbrace{r^n \equiv 1 \pmod{2p^k}} \Longrightarrow n \mid \varphi(2p^k) = \varphi(2)\varphi(p^k)$$
$$= \varphi(p^k) = p^{k-1}(p-1)$$

$$\Longrightarrow r^n \equiv 1 \pmod{p} \Longrightarrow p-1 \mid n.$$

$$\Longrightarrow n = \varphi(2p^k).$$

$\square$

Let n be an integer with a primitive root r.

Then $\{r, r^2, \dots, r^{\varphi(n)}\} \equiv$ integers $< n$ that are relatively prime to n

Given a s.t. $\gcd(a,n)=1$, let k be the <u>smallest</u> exponent s.t. $a \equiv r^k \pmod n$. Then k is the <u>index</u> of a relative to r, denoted $\operatorname{ind}_r a$ or $\operatorname{ind} a$.

<u>Properties</u>: (1) $\operatorname{ind}(ab) \equiv \operatorname{ind}(a) + \operatorname{ind}(b) \pmod{\varphi(n)}$

(2) $\operatorname{ind}(a^k) \equiv k \cdot \operatorname{ind}(a) \pmod{\varphi(n)}$

<u>pf.</u>: (1) $a \equiv r^{\operatorname{ind} a} \pmod n$, $b \equiv r^{\operatorname{ind} b} \pmod n \Longrightarrow ab \equiv r^{\operatorname{ind} a + \operatorname{ind} b} \pmod n$

and $ab \equiv r^{\operatorname{ind}(ab)} \pmod n$. Thus, $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b$ modulo $\varphi(n)$.

(2) $r^{\operatorname{ind}(a^k)} \equiv a^k$, $(r^{\operatorname{ind} a})^k \equiv a^k \Longrightarrow \operatorname{ind}(a^k) \equiv k \cdot \operatorname{ind} a \mod \varphi(n)$. $\boxtimes$

__Thus:__ $x^k \equiv a \pmod{n} \iff \operatorname{ind}(x^k) \equiv \operatorname{ind} a \pmod{\varphi(n)}$

$$\text{i.e. } \underbrace{k(\operatorname{ind} x) \equiv \operatorname{ind} a \pmod{\varphi(n)}}$$

solvable iff $d := \gcd(k, \varphi(n))$ divides $\operatorname{ind} a$; if $d \mid \operatorname{ind} a$, there are d solutions.

$k = 2$, $n = p = \overset{\text{odd}}{\text{prime}}$: $x^2 \equiv a \pmod{p} \iff 2 \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}$,

solvable iff $\gcd(2, p-1) = 2 \mid \operatorname{ind} a$; if $2 \mid \operatorname{ind} a$, there are 2 solutions.

There are solutions for $a \equiv \underbrace{r^2, r^4, \ldots, r^{p-1}}$

$\frac{p-1}{2}$ such a, i.e., there are $\frac{p-1}{2}$ quadratic residues.

<u>example</u> $n = 17$, $\varphi(17) = 16$

primitive root: $2 \equiv 2$, $2^2 \equiv 4$, ~~8~~ $\underset{\equiv -1}{2^4 \equiv 16}$, $\underline{\underline{2^8 \equiv 1}}$ ✓

2 is <u>not</u> a primitive root of 17

$3 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 81 \equiv 13$, $3^8 \equiv 169 \equiv -1$,

$3^{16} \equiv 1 \implies 3$ is a primitive root.

$n = 17$

$\underline{\underline{r = 3}}$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ind a	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27 \equiv 10$, $3^4 \equiv 30 \equiv 13$, $3^5 \equiv 39 \equiv 5$,

$3^6 \equiv 15$, $3^7 \equiv 45 \equiv 11$, $3^8 \equiv 33 \equiv 16$, $3^9 \equiv 48 \equiv 14$, $3^{10} \equiv 42 \equiv 8$

$3^{11} \equiv 24 \equiv 7$, $3^{12} \equiv 21 \equiv 4$, $3^{13} \equiv 12$, $3^{14} \equiv 36 \equiv 2$, $3^{15} \equiv 6$

31(a) $x^{12} \equiv 13 \pmod{17}$

$\iff 12 \cdot \operatorname{ind} x \equiv \operatorname{ind} 13 \pmod{16}$

$\iff 12 \cdot \operatorname{ind} x \equiv 4 \pmod{16}$

$\iff 3 \cdot \operatorname{ind} x \equiv 1 \pmod{4} \iff 3 \operatorname{ind} x = 4k+1$

$\operatorname{ind} x = 3, 7, 11, 15$

$\boxed{x = 10, 11, 7, 6}$

31(b) $8x^5 \equiv 10 \pmod{17}$

$\operatorname{ind}(8x^5) \equiv \operatorname{ind} 10 \pmod{16}$

$\operatorname{ind} 8 + 5 \operatorname{ind} x \equiv 3 \pmod{16}$

$10 + 5 \operatorname{ind} x \equiv 3 \pmod{16}$

$5 \operatorname{ind} x \equiv 9 \pmod{16}$

$5 \operatorname{ind} x = 16k + 9$

$\operatorname{ind} x = 5 \implies x = 5$

FACT: The congruence $x^k \equiv a \pmod{n}$

is solvable iff $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{\cancel{\varphi(n)}\, n}$, $d = \gcd(k, \varphi(n))$.

pf.: $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{\cancel{\varphi(n)}\, n}$

$\iff \frac{\varphi(n)}{d} \cdot \operatorname{ind} a \equiv 0 \pmod{\varphi(n)}$

$\varphi(n) \cdot \left(\frac{\operatorname{ind} a}{d}\right) \equiv 0 \pmod{\varphi(n)}$ $\iff k \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\varphi(n)}$

$\iff \frac{\operatorname{ind} a}{d} \in \mathbb{N}$, i.e., $d \mid \operatorname{ind} a$. $\iff x^k \equiv a \pmod{n}$.

$\boxed{}$

Corollary $k = 2$, $n = \text{prime } p$:

$\underline{x^2 \equiv a \pmod{p}}$ solvable iff $\underbrace{\underline{a^{\frac{p-1}{2}}} \equiv 1 \pmod{\cancel{\ }\, p}}_{\text{Euler's criterion}}$.

<u>Euler's criterion</u>