$a, n \in \mathbb{N}$, $\gcd(a,n) = 1$

order of a mod n : smallest exponent k s.t.

$$a^k \equiv 1 \pmod{n}$$

example order of 2 mod 17 :

$$2,\ 2^2 \equiv 4,\ 2^3 = 8,\ 2^4 \equiv 16,\ 2^5 \equiv 15,\ 2^6 \equiv 13,\ 2^7 \equiv 9,\ \boxed{2^8 \equiv 1}$$

order of 2 mod 17 is 8 ; Euler: $2^{16} \equiv 1 \pmod{17}$

---

recall: order of 2 mod 27 is $\varphi(27) = 18$ (#12, 7.4)

---

a is a primitive root of n if its order mod n is $\varphi(n)$.

Thus, 2 is a primitive root of 27.

FACTS $\gcd(a,n)=1$, k = order of a mod n

Then $a^h \equiv 1 \pmod n$ iff $k \mid h$.

pf. if $k \mid h$, then $(a^k)^{\frac{h}{k}} = a^h \equiv 1 \pmod n$.

if $a^h \equiv 1 \pmod n$, then $h = qk + r$, $0 \le r \le k-1$

and $a^h = a^{qk} a^r \equiv a^r \equiv 1 \pmod n \Rightarrow r = 0$,

$k \mid h$.

If $h > 0$ is given, then the order of a^h is $\frac{k}{\gcd(h,k)}$.

pf. Let $d = \gcd(h,k)$, so that $h = h_1 d$ and $k = k_1 d$ with

h_1, k_1 relatively prime. Then $(a^h)^{k_1} = (a^{h_1 d})^{\frac{k}{d}} = a^{hk_1} \equiv 1$.

If r = order of a^h mod n, then $r \mid k_1$.

$(a^h)^r = a^{hr} \equiv 1 \pmod n \Rightarrow k \mid hr$, so $k_1 d \mid h_1 d r$, $k_1 \mid h_1 r \Rightarrow k_1 \mid r$. $\Uparrow$ $r = k_1$ $\Leftarrow$

Corollary: a and a^k have the same order if $\gcd(k, k) = 1$, k = order of a.

FACT: if a is a primitive root of n, then

$$\{a, a^2, \ldots, a^{\varphi(n)}\} \equiv \{a_1, a_2, \ldots, a_{\varphi(n)}\}$$

the $\varphi(n)$ integers less than n and relatively prime to n

pf. if $a^i \equiv a^j \pmod n \Rightarrow a^{i-j} \equiv 1 \pmod n$

$\Rightarrow k \mid i-j \Rightarrow i \equiv j \pmod k$

$\Rightarrow i = j$. .

Theorem If n has a primitive root, then it has exactly $\varphi(\varphi(n))$ of them.

pf. Let a be a primitive root of n. Then

$\{a, a^2, \ldots, a^{\varphi(n)}\}$ are incongruent mod n.

of these, $\varphi(\varphi(n))$ of the exponents are relatively prime to $\varphi(n)$.

$\square$

8.1 11(a) primitive roots of 10:

$\varphi(10) = \varphi(2)\varphi(5) = \underline{4}$; $\{a_1, a_2, a_3, a_4\} = \{1, 3, 7, 9\}$

$3 \equiv 3$, $3^2 \equiv 9 \equiv -1$, $3^4 \equiv 1 \pmod{10} \Rightarrow$ 3 is a primitive root of 10

$7 \equiv 7$, $7^2 = 49 \equiv -1$, $7^4 \equiv 1 \pmod{10} \Rightarrow$ 7 is a primitive root of 10

$3^4 \equiv 1 \pmod{10}$ is equivalent to $9^2 \equiv 1 \pmod{10}$, so 9 is not a primitive root of 10

11(b) 3 is a primitive root of 17: $3 \equiv 3$, $3^2 \equiv 9$, $3^4 = 81 \equiv 13$, $3^8 \equiv 169 \equiv -1$, $3^{16} \equiv 1$ ✓

Thus, 17 has $\varphi(\varphi(17)) = \varphi(16) = \underline{8}$ primitive roots.

To find them, extract the powers 3^k of 3 with $\gcd(k, 16) = 1$:

$\{3, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15}\}$ are the 8 primitive roots of 17.

$3^3 \equiv 10$, $3^5 \equiv 5$, $3^7 \equiv 11$, $3^9 \equiv 14$, $3^{11} \equiv 7$, $3^{13} \equiv 12$, $3^{15} \equiv 6$

$\Rightarrow \{3, 5, 6, 7, 10, 11, 12, 14\}$ are the primitive roots < 17.

$\gcd(a,n)=1$, order of a mod n is k: $a^k \equiv 1 \pmod n$

a is a primitive root of n if $k = \varphi(n)$

---

* $\{a, a^2, \dots, a^k\}$ are all incongruent mod n
* if n has a primitive root, then it has $\varphi(\varphi(n))$ of them
* if $h>0$, then the order of a^h is k iff $\gcd(h,k)=1$

---

primitive roots of 19: Fermat $\Longrightarrow a^{18} \equiv 1 \pmod{19}$, $1 \le a \le 18$

$a=2$: 2, $2^2=4$, $2^3=8$, $2^6=64 \equiv 7 \pmod{19}$, $2^9 \equiv 56 \equiv -1$

$\Longrightarrow 2^{18} \equiv 1$, 2 is a primitive root of 19.

others: 2^h s.t. $\gcd(h,18)=1 \Longrightarrow 1, 5, 7, 11, 13, 17$

↳ $2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$

$\varphi(\varphi(19)) = \varphi(18) = \varphi(2)\varphi(9) = 6$

Legendre's Thm p a prime

$\hookrightarrow$ $f(x) = a_n x^n + \dots + a_1 x + a_0$, $\gcd(a_n, p) = 1$.

$\hookrightarrow$ $f(x) \equiv 0 \pmod p$ has at most n solutions.

pf. base case $n=1$: $f(x) = a_1 x + a_0$, $a_1 x + a_0 \equiv 0 \pmod p$

i.e., $a_1 x \equiv -a_0 \pmod p \Longrightarrow \exists!$ solution.

IH: suppose true for f of degree $n-1$, some $n \geq 2$.

Let $f(x) = a_n x^n + \dots + a_1 x + a_0$, and let a satisfy

$f(a) \equiv 0 \pmod p$. Then $f(x) = (x-a)q(x) + r$, and

$f(a) \equiv 0 \pmod p \iff r \equiv 0 \pmod p \Longrightarrow f(x) \equiv (x-a)q(x)$.

If there's another soln b, $b \not\equiv a \pmod p$, then

$0 \equiv f(b) \equiv (b-a)q(b) \pmod p \Longrightarrow q(b) \equiv 0 \pmod p$.

$\Longrightarrow$ There are at most $(n-1)$ b's. ∎

Thm p prime, $d \mid p-1 \Longrightarrow$ There are exactly d solutions of $x^d \equiv 1 \pmod p \iff x^d - 1 \equiv 0 \pmod p$.

pf. Fermat: $x^{p-1} \equiv 1 \pmod p$ has $(p-1)$ solns, $1, 2, \dots, p-1$.

$$\underbrace{x^{p-1} - 1}_{\substack{p-1 \text{ solns} \\ \equiv 0}} = \underbrace{(x^d - 1)}_{\substack{\text{at least} \\ d \text{ solns}}} \underbrace{(x^{p-1-d} + x^{p-1-d-1} + \dots + x + 1)}_{\text{at most } p-1-d \text{ solutions, } \equiv 0}$$

$\Downarrow$

has exactly d solns!

Thm p prime, $d \mid p-1 \Rightarrow$ There are $\varphi(d)$ integers of order d. (in $1 \le \dots \le p-1$)

pf. $\psi(d) = \#$ integers $\le p-1$ of order d.

$$p-1 = \sum_{d \mid p-1} \psi(d) \quad \text{by Fermat.}$$

$$p-1 = \sum_{d \mid p-1} \varphi(d) \quad \text{by Gauss.}$$

Will prove that $\psi(d) \le \varphi(d)$ $\forall$ d.

$\psi(d) = 0 \Rightarrow \psi(d) < \varphi(d)$

$\psi(d) > 0 \Rightarrow$ There is some a of order d, and $\{a, a^2, \dots, a^d\}$ are incongruent mod p.
and $(a^h)^d = (a^d)^h \equiv 1 \pmod p$
And $\varphi(d)$ of these have order d. $\Rightarrow \psi(d) = \varphi(d)$. ∎

Corollary: p prime $\Rightarrow$ there are $\varphi(p-1)$ primitive roots of p.

4(a) 3 is a primitive root of 43. $\varphi(43) = 42$

Find integers having order 6. $\Rightarrow \varphi(6) = \varphi(2)\varphi(3) = 2$

(There are 2 of them.)

$\{3, 3^2, \ldots, 3^{42}\}$ incongruent mod 43.

3^h has order 6 iff $\frac{42}{\gcd(42,h)} = 6$ iff $\gcd(42,h) = 7$.

$h = 7, 21 \Rightarrow 3^7, 3^{21}$.

Thm $\gcd(m,n)=1$; $m,n>2$

Then mn does not have a primitive root.

Pf. Let $\underbrace{d=\gcd(\varphi(m),\varphi(n))}$, $h=\operatorname{lcm}(\varphi(m),\varphi(n))$.

$d\geq 2 \Longrightarrow \frac{1}{d}\leq\frac{1}{2}$, and

$$h=\frac{\varphi(m)\varphi(n)}{d}\leq\frac{\varphi(mn)}{2}$$

Let a be rel. prime to mn. Then

$$a^{\varphi(m)}\equiv 1 \pmod n \Longrightarrow \left(a^{\varphi(m)}\right)^{\frac{\varphi(n)}{d}} = a^{h}\equiv 1 \pmod m$$

and $a^{h}\equiv 1 \pmod n \longrightarrow a^{h}\equiv 1 \pmod{mn}$.

∎