Review. $x \pmod{n}$ is a primitive root.

$\iff$ The (multiplicative) order of $x \pmod{n}$ is $\phi(n)$. (That is, the order is as large as possible.)

$\iff$ $x, x^2, \ldots, x^{\phi(n)}$ is a list of all invertible residues modulo n.

Example 118. Is there a primitive root modulo 8?

Solution. Since $\phi(8) = 8 - 4 = 4$, the question is whether there is a residue of order 4.
The invertible residues are $\pm 1, \pm 3$. Obviously, 1 has order 1 and -1 has order 2. Since $(\pm 3)^2 \equiv 1 \pmod{8}$, the residues ± 3 have order 2 as well. There is no primitive root.

Lemma 119. If $a^r \equiv 1 \pmod{n}$ and $a^s \equiv 1 \pmod{n}$, then $a^{\gcd(r,s)} \equiv 1 \pmod{n}$.

Proof. By Bezout's identity, there are integers x, y such that $xr + ys = \gcd(r, s)$.
Hence, $a^{\gcd(r,s)} = a^{xr+ys} = a^{xr} a^{ys} = (a^r)^x (a^s)^y \equiv 1 \pmod{n}$. □

Corollary 120. The multiplicative order of a modulo n divides $\phi(n)$.

Proof. Let k be the multiplicative order, so that $a^k \equiv 1 \pmod{n}$. By Euler's theorem $a^{\phi(n)} \equiv 1 \pmod{n}$. The previous lemma shows that $a^{\gcd(k,\phi(n))} \equiv 1 \pmod{n}$. But since the multiplicative order is the smallest exponent, it must be the case that $\gcd(k, \phi(n)) = k$. Equivalently, k divides $\phi(n)$. □

Example 121. Determine the orders of each (invertible) residue modulo 7. In particular, determine all primitive roots modulo 7.

Solution. First, observe that, since $\phi(7) = 6$, the orders can only be $1, 2, 3, 6$. Indeed:

residue	1	2	3	4	5	6
order	1	3	6	3	6	2

The primitive roots are 3 and 5.

Lemma 122. Suppose $x \pmod{n}$ has (multiplicative) order k.

(a) $x^a \equiv 1 \pmod{n}$ if and only if $k | a$.

(b) $x^a \equiv x^b \pmod{n}$ if and only if $a \equiv b \pmod{k}$.

(c) x^a has order $\frac{k}{\gcd(k, a)}$.

Proof.

(a) "$\Longrightarrow$": By Lemma 119, $x^k \equiv 1$ and $x^a \equiv 1$ imply $x^{\gcd(k,a)} \equiv 1 \pmod{n}$. Since k is the smallest exponent, we have $k = \gcd(k, a)$ or, equivalently, $k | a$.
"$\Longleftarrow$": Obviously, if $k | a$ so that $a = kb$, then $x^a = (x^k)^b \equiv 1 \pmod{n}$.

(b) Since x is invertible, $x^a \equiv x^b \pmod{n}$ if and only if $x^{a-b} \equiv 1 \pmod{n}$ if and only if $k | (a - b)$.

(c) By the first part, $(x^a)^m \equiv 1 \pmod{n}$ if and only if $k | am$. The smallest such m is $m = \frac{k}{\gcd(k, a)}$. □

Example 123. Redo Example 121, starting with the knowledge that 3 is a primitive root.

Solution.

residues	1	2	3	4	5	6
3^a	3^0	3^2	3^1	3^4	3^5	3^3
order$=\frac{6}{\gcd(a,6)}$	$\frac{6}{6}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{3}$

Armin Straub
straub@southalabama.edu