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.

Lemma 123. 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 124. 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 125. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Solution.

- $2 \pmod{7}$: $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  Since the order is less than $\phi(7) = 6$, 2 is not a primitive root modulo 7.
- $2 \pmod{11}$: Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.
  Since the order is equal to $\phi(11) = 10$, 2 is a primitive root modulo 11.
- $2 \pmod{9}$: Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)
  Since the order is equal to $\phi(9) = 6$, 2 is a primitive root modulo 9.
- The order of $2 \pmod{15}$ is 4 (a divisor of $\phi(15) = 8$).
  2 is not a primitive root modulo 15. In fact, there is no primitive root modulo 15.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Advanced comment. There exists a primitive root modulo n if and only if n is of one of $1, 2, 4, p^k, 2p^k$ for some odd prime p.

Example 126. 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.

Armin Straub
straub@southalabama.edu

Lemma 127. 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 123, $x^k \equiv 1$ 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 128. Redo Example 122, starting with the knowledge that 3 is a primitive root.

That is, determine the orders of each residue modulo 7.

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