PROPOSITION: Let p be a prime. Let $p(x)$ be a polynomial of degree d with coefficients in $\mathbb{Z}_p$. Then $p(x)$ has at most d roots in $\mathbb{Z}_p$. $\square$

LEMMA (FROM HW): If G is a group, $g \in G$, and n a positive integer such that $g^n = 1$, then the order of g divides n.

DEFINITION: Let n be a positive integer. An element $g \in \mathbb{Z}_n^\times$ is a **primitive root** if the order of g in $\mathbb{Z}_n^\times$ equals $\phi(n)$ (the cardinality of $\mathbb{Z}_n^\times$).

THEOREM: Let p be a prime number. Then there exists a primitive root in $\mathbb{Z}_p^\times$.

(1) Warmup with primitive roots:
   (a) Check that $[2]$ is a primitive root in $\mathbb{Z}_5$.
   (b) Check that $[3]$ is a primitive root in $\mathbb{Z}_4$.
   (c) Find a primitive root in $\mathbb{Z}_7$.
   (d) Show that there is no primitive root in $\mathbb{Z}_8$.

   (a) $\varphi(5) = 4$ so we want order 4. $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$, $[2]^4 = [1]$, so the order of $[2]$ is indeed 4.
   (b) $\varphi(4) = 2$ so we want order 2. $[3]^1 = [2]$, $[3]^2 = [1]$, so the order of $[3]$ is indeed 2.
   (c) $[2]$ doesn't work, since $[2]^3 = [1]$, but $[3]$ is a primitive root.
   (d) $[3]^2 = [5]^2 = [7]^2 = [1]$, so nothing has order $4 = \varphi(8)$.

(2) Suppose that $g = [a]$ is a primitive root in $\mathbb{Z}_p$.
   (a) Show that[1] if $0 \le m \le n < p-1$, and $g^m = g^n$, then $m = n$.
   (b) Show that every element of $\mathbb{Z}_p^\times$ can be written as g^n for a unique integer n with $0 \le n < p-1$.
   (c) Show that the relation $y \in \mathbb{Z}_p^\times \rightsquigarrow [m] \in \mathbb{Z}_{p-1}$ if $y = g^m$ is a well-defined function $I : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$.

   (a) Let $0 \le m \le n < p-1$ and $x^m = x^n$. Then $[1] = x^{-m}x^m = x^{-m}x^n = x^{n-m}$ and $n - m < p-1$. Since the order of x is $p-1$, we must have $n - m = 0$, so $n - m$.
   (b) From part (1), $\{1, x, x^2, \dots, x^{p-2}\}$ are distinct elements of $\mathbb{Z}_p^\times$. Since this list has $p-1$ elements and $\mathbb{Z}_p^\times$ does too, each element of $\mathbb{Z}_p^\times$ must occur exactly once.
   (c) We need to show that if $y = g^m = g^n$, then $[m] = [n]$ in $\mathbb{Z}_{p-1}$. Say $m \le n$. If $g^m = g^n$, then $1 = g^{n-m}$, so by the lemma, $p-1 \mid n-m$, and hence $n \equiv m \pmod{p-1}$; i.e., $[m] = [n]$ in $\mathbb{Z}_{p-1}$.

DEFINITION: If $[a]$ is a primitive root in $\mathbb{Z}_p$, the function

$$\mathbb{Z}_p^\times \to \mathbb{Z}_{p-1} \quad [b] \mapsto [m] \text{ such that } [b] = [a]^m$$

is called the **discrete logarithm** or **index** of $\mathbb{Z}_p^\times$ with base $[a]$.

(3) Let p be a prime and $[a]$ a primitive root in $\mathbb{Z}_p$. Show that the corresponding discrete logarithm function $I : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$ satisfies the property

$$I(xy) = I(x) + I(y) \quad \text{and} \quad I(x^n) = [n]I(x)$$

[1] Hint: x^m has an inverse.

for $x, y \in \mathbb{Z}_p^\times$ and $n \in \mathbb{N}$.

Let $x, y \in \mathbb{Z}_p^\times$, and say that $I(x) = [\ell]$ and $I(y) = [m]$. Then $x = [a]^\ell$ and $y = [a]^m$. So, $xy = [a]^\ell [a]^m = [a]^{\ell+m}$, and hence $I(xy) = [\ell + m] = I(x) + I(y)$.

Similarly, since $x^n = [a]^{\ell n}$, $I(x^n) = [\ell n] = [n][\ell] = [n]I(x)$.

(4) (a) Verify that $[2]$ is a primitive root in $\mathbb{Z}_{11}$ and compute the corresponding discrete logarithm.
(b) Use this function to find a square root of $[3]$ in $\mathbb{Z}_{11}$.

(a) Compute the powers of $[2]$:

n	0	1	2	3	4	5	6	7	8	9
$[2]^n$	$[1]$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$

and $[2]^{10} = [1]$. The index function is just the inverse function:

x	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$I(x)$	0	1	8	2	4	9	7	3	6	5

(b) Since $I([3]) = 8$, an element of index 4 would be a square root, so $[5]$ is a square root.

PROPOSITION: Let n be a positive integer. Then $\sum_{d \mid n} \varphi(d) = n$.

THEOREM: Let p be a prime. Suppose that there are n distinct solutions to $x^n = 1$ in $\mathbb{Z}_p$. Then $\mathbb{Z}_p^\times$ has exactly $\varphi(n)$ elements of order n.

(5) Explain how the theorem above implies that there exists a primitive root in $\mathbb{Z}_p$.

By FLT, every element of $\mathbb{Z}_p^\times$ is a solution to $x^{p-1} = 1$ in $\mathbb{Z}_p$, so the theorem applies. There are then $\varphi(p-1)$ elements of order $p-1$ in $\mathbb{Z}_p^\times$. Since $\mathbb{Z}_{p-1}^\times$ is nonempty, $\varphi(p-1) > 0$. Thus, there is a primitive root.

(6) Proof of Theorem (using the Proposition): Fix a prime number p.
(a) We proceed by strong induction on n. What does that mean concretely here? Complete the case $n = 1$.
(b) Suppose that $x^n = 1$ but the order of x in $\mathbb{Z}_p^\times$ is not n. What does the Lemma say about the order of x? Rephrase this in terms of x satisfying an equation.
(c) Suppose that d is a divisor of n, and write $n = de$. Note that

$$x^n - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1).$$

In particular, every solution of $x^n - 1$ is a root of $x^d - 1$ or of $x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1$. Can $x^d - 1$ have more than d roots in $\mathbb{Z}_p$? Can $x^d - 1$ have less than d roots in $\mathbb{Z}_p$ if $x^n - 1$ has n roots?
(d) Apply the induction hypothesis to show that the number of solutions to $x^n = 1$ of order *less than* n is $\sum_{d \mid n, d \neq n} \varphi(d)$.
(e) Apply the Proposition to conclude the proof of the Theorem.

(a) We must show that it is true for $n = 1$ and that if, for each $d < n$, if $x^d = 1$ has d distinct solutions then there are $\varphi(d)$ elements of order d in $\mathbb{Z}_p^\times$, then if $x^n = 1$ has n distinct solutions then there are $\varphi(n)$ elements of order n in $\mathbb{Z}_p^\times$. Henceforth, we will assume that, for each $d < n$, if $x^d = 1$ has d distinct solutions then there are $\varphi(d)$ elements of order d in $\mathbb{Z}_p^\times$.

(b) The order of x divides n in this case. That is, x is a root of $x^d - 1$.

(c) No, by the first theorem, $x^d - 1$ cannot have more than d roots in $\mathbb{Z}_p$. If $x^n - 1$ has n roots, note that $x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1$ has at most $d(e-1) = n - d$ roots. If $x^d - 1$ had $c < d$ roots, then $x^n - 1$ would have at most $c + (n - d) < d + n - d = n$ roots, contradicting the hypothesis.

(d) The IH applies to every divisor d of n, so for each $d \mid n$, $d < n$, we have $\varphi(d)$ elements of order d.

(e) The total number of solutions to $x^n - 1$ is n. Every such solution either has order n or order d with $d \mid n$ and $d < n$. Adding up all of the latter type gives

$$\sum_{d \mid n, d \neq n} \varphi(d) = \left(\sum_{d \mid n} \varphi(d) \right) - \varphi(n) = n - \varphi(n).$$

Thus, the number of solutions with order n is $\varphi(n)$.

(7) Proof of Proposition:

(a) Explain the following formula:

$$n = \sum_{d \mid n} \#\{a \mid 1 \le a \le n \text{ and } \gcd(a, n) = d\}.$$

(b) Explain[2] why

$$\#\{a \mid 1 \le a \le n \text{ and } \gcd(a, n) = d\} = \varphi(n/d).$$

(c) Finally, explain[3] why

$$\sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$$

and complete the proof.

(a) Every integer between 1 and n occurs in exactly one of the sets on the right hand side.

(b) Following the hint, the integers between 1 and n whose gcd with n is d correspond to integers between 1 and n/d that are coprime with n/d. The phi function counts the latter.

(c) As d ranges through the divisors of n, n/d goes through all of the divisors of n, obtaining each value once. Put together with the previous parts, the formula follows.

(8) Let p, q be distinct odd primes. Show that there is no primitive root of $\mathbb{Z}_{pq}$: i.e., there is no element of order $\varphi(pq)$ in $\mathbb{Z}_{pq}^\times$.

[2]Hint: You proved that if $\gcd(a, n) = d$, then $\gcd(a/d, n/d) = 1$; also, if $\gcd(b, n/d) = 1$, then $\gcd(bd, n) = d$.

[3]Hint: As d ranges through all the divisors of n, so does n/d.