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 $\mathbb{Z}_p$. □

DEFINITION: Let n be a positive integer. An element $x \in \mathbb{Z}_n^\times$ is a **primitive root** if the order of x 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 $\mathbb{Z}_8$.

(2) Suppose that $x = [a]$ is a primitive root in $\mathbb{Z}_p$.
  (a) Show that[1] if $0 \leq m \leq n < p-1$, and $x^m = x^n$, then $m = n$.
  (b) Show that every element of $\mathbb{Z}_p^\times$ can be written as x^n for a unique integer n with $0 \leq n < p-1$.

If $[a]$ is a primitive root in $\mathbb{Z}_p$, then every nonzero element of $\mathbb{Z}_p$ can be written as $[a]^m$ for a unique nonnegative integer $m < p-1$. We call the function

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

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

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

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

(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 $\mathbb{Z}_{11}$.

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

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 $\mathbb{Z}_p$.

(6) Proof of Theorem (using the Proposition): Fix a prime number p. We will use the following LEMMA: 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.

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

(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.

(7) Proof of Proposition:

(a) Explain the following formula:

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

(b) Explain[2] why

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

(c) Finally, explain[3] why

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

and complete the proof.

(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.