

THE GENERAL PRIMITIVE ROOT THEOREM

We showed in class that if p is prime, then there exist primitive roots mod p . For *odd* primes p , we will now show that there exist primitive roots modulo p^k and $2p^k$ for all $k \geq 1$. We will write $\text{ord}_n(a)$ instead of $e_n(a)$ for the order of a modulo n . Recall that an integer g with $(g, n) = 1$ is a primitive root modulo n if and only if $\text{ord}_n(a) = \phi(n)$.

Theorem 1. *Let p be an odd prime.*

- (a) *If g is a primitive root mod p , then either g or $g + p$ is a primitive root mod p^2 .*
- (b) *If g is a primitive root mod p^2 , then g is a primitive root mod p^k for all $k \geq 2$.*
- (c) *If g is a primitive root mod p^k for some $k \geq 1$, then either g or $g + p^k$ is a primitive root mod $2p^k$.*

Proof. (a) If $m = \text{ord}_{p^2}(g)$, then we know that $m \mid p(p-1)$. Since $g^m \equiv 1 \pmod{p^2}$, we also have $g^m \equiv 1 \pmod{p}$, and thus (since g is a primitive root mod p) $p-1 \mid m$. It follows that either $m = p-1$ or $m = p(p-1)$. The same reasoning applies to $m' = \text{ord}_{p^2}(g+p)$, since $g+p$ is also a primitive root mod p , so $m' = p-1$ or $m' = p(p-1)$. Suppose that $m = m' = p-1$. From $m' = p-1$, we see that

$$(g+p)^p \equiv (g+p)(g+p)^{p-1} \equiv g+p \pmod{p^2}. \quad (1)$$

By the binomial theorem,

$$(g+p)^p \equiv g^p \pmod{p^2}. \quad (2)$$

And since $m = p-1$, we have $g^{p-1} \equiv 1 \pmod{p^2}$, so that

$$g^p \equiv g \pmod{p^2}. \quad (3)$$

Combining equations (1)-(3), we have $g + p \equiv g \pmod{p^2}$, which implies that $p \equiv 0 \pmod{p^2}$, a contradiction. Therefore either $m = p(p-1)$ or $m' = p(p-1)$, which is equivalent to the statement that either g or $g + p$ is a primitive root mod p^2 .

(b) By induction on k , it suffices to prove that if g is a primitive root mod p^k ($k \geq 2$), then g is a primitive root mod p^{k+1} . Let $m = \text{ord}_{p^{k+1}}(g)$, so that $m \mid \phi(p^{k+1}) = (p-1)p^k$. Since $g^m \equiv 1 \pmod{p^{k+1}}$, we also have $g^m \equiv 1 \pmod{p^k}$. As g is a primitive root mod p^k , this implies that $\phi(p^k) = (p-1)p^{k-1} \mid m$. Thus $m = (p-1)p^{k-1}$ or $m = (p-1)p^k$. So to prove that g is a primitive root mod p^{k+1} , it suffices to show that

$$g^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}. \quad (4)$$

To prove (4), note first that since $g^{(p-1)p^{k-2}} \equiv 1 \pmod{p^{k-1}}$ by Euler's theorem, we can write

$$g^{(p-1)p^{k-2}} = 1 + ap^{k-1} \quad (5)$$

for some $a \in \mathbf{Z}$. If we raise both sides of (5) to the p th power, then by the binomial theorem we have

$$\begin{aligned} g^{(p-1)p^{k-1}} &= 1 + \binom{p}{1}ap^{k-1} + \binom{p}{2}a^2p^{2k-2} + \dots + \binom{p}{p}a^p p^{p(k-1)} \\ &\equiv 1 + ap^k \pmod{p^{k+1}}. \end{aligned}$$

(This is the only place where we use the fact that p is odd, since if $p = 2$ and $k = 2$ the term $\binom{p}{p}a^p p^{p(k-1)}$ need not be divisible by p^{k+1} .)

If $g^{(p-1)p^{k-1}} \equiv 1 \pmod{p^{k+1}}$, we deduce that $ap^k \equiv 0 \pmod{p^{k+1}}$, so that $p \mid a$. But then (5) implies that $g^{(p-1)p^{k-2}} \equiv 1 \pmod{p^k}$, contradicting the fact that g is assumed to be a primitive root mod p^k . This proves (4), and hence part (b) of the theorem.

(c) Note first that $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$. Let $m = \text{ord}_{2p^k}(g)$. If g is odd, then g is relatively prime to $2p^k$ and Euler's theorem implies that $m \mid \phi(2p^k) = \phi(p^k)$. On the other hand, if $g^m \equiv 1 \pmod{2p^k}$ then $g^m \equiv 1 \pmod{p^k}$ as well. Since g is a primitive root mod p^k , we have $\phi(p^k) \mid m$. Thus $m = \phi(2p^k)$ and g is a primitive root mod $2p^k$. If g is even, then $g + p^k$ is odd and is also a primitive root mod p^k , so by the same reasoning $g + p^k$ is then a primitive root mod $2p^k$. \square

Since -1 is a primitive root modulo 2 and 4, the theorem implies that if $n = 2, 4, p^k$, or $2p^k$, where p is an odd prime, then there exists a primitive root mod n . Conversely, we have:

Theorem 2 (Primitive Root Theorem). *Let $n \geq 2$ be a positive integer. There exist primitive roots modulo n iff $n = 2, 4, p^k$, or $2p^k$, where p is an odd prime.*

Proof. We showed in class that if $(a, n) = 1$, with a and n positive integers, then $a^{\lambda(n)} \equiv 1 \pmod{n}$. Here if $n = 2^a p_1^{e_1} \cdots p_k^{e_k}$, we define

$$\lambda(n) = \text{LCM}(\psi(2^a), \phi(p_1^{e_1}), \dots, \phi(p_k^{e_k}))$$

where $\psi(2^a) = \phi(2^a)$ if $0 \leq a \leq 2$ and $\psi(2^a) = \frac{1}{2}\phi(2^a)$ if $a \geq 3$. It follows that $\lambda(n) \mid \phi(n)$, and if $\lambda(n) < \phi(n)$ then there are no primitive roots mod n . Since it is easy to check that for $n \geq 2$, $\lambda(n) = \phi(n)$ iff $n = 2, 4, p^k$, or $2p^k$, where p is an odd prime, the theorem is proved. \square