Math 445 Number Theory

October 1, 2004

Theorem: If p is an odd prime and $k \geq 1$, then $m = p^k$ has a primitive root, i.e., there is an integer b with $\mathrm{ord}_{p^k}(b) = \Phi(p^k) = p^{k-1}(p-1)$.

We have so far shown this to be true for $k = 1, 2$. Today we see:

If p is an odd prime and b is a primitive root mod p^2, then b is a primitive root mod p^k for all $k \geq 1$. In fact, we will show:

(*) If p is an odd prime and, for $k \geq 1$, $\mathrm{ord}_{p^{k+1}}(b) > \mathrm{ord}_{p^k}(b)$, then $\mathrm{ord}_{p^{k+m}}(b) = p^m \cdot \mathrm{ord}_{p^k}(b)$ for all $m \geq 1$.

To see this, set $\alpha = \mathrm{ord}_{p^{k+1}}(b)$ and $\beta = \mathrm{ord}_{p^k}(b)$, then $b^\alpha \equiv 1 \pmod{p^{k+1}}$ implies $b^\alpha \equiv 1 \pmod{p^k}$, so $\alpha|\beta$, while $p^k | b^\beta - 1$ and $p^{k+1} \not| b^\beta - 1$ (since $\alpha > \beta$ implies $b^\beta = 1 + sp^k$ with $p^{k+1} \not| sp^k$, so $p \not| s$, so $(s,p) = 1$. But then, mod p^{k+1}

$$b^{p\beta} = (1+sp^k)^p = 1 + psp^k + \binom{p}{2} s^2 p^{2k} + \binom{p}{3} s^3 p3k + \cdots = 1 + p^{k+1}(s + \frac{p-1}{2} s^2 p^k + \binom{p}{3} s^3 p^{2k-1} + \cdots) = 1 + p^{k+1}(s + p(\frac{p-1}{2} s^2 p^{k-1} + \binom{p}{3} s^3 p^{2k-2} + \cdots))1 + p^{k+1}s' \equiv 1$$

so $\alpha | p\beta$, so $\alpha = \beta$ (contradicting our hypothesis) or $\alpha = p\beta$. So $\alpha = p\beta$. But even more, since $s + p(\frac{p-1}{2} s^2 p^{k-1} + \binom{p}{3} s^3 p^{2k-2} + \cdots \equiv s \pmod{p}$, so $(s', p) = 1$, we have $b^{p\beta} \not\equiv 1 \pmod{p^{k+2}}$ (since $p^{k+2} \not| s' p^{k+1}$) . So $\mathrm{ord}_{p^{k+2}}(b) > \mathrm{ord}_{p^{k+1}}(b)$. So we can start the exact same argument over again, to show that $\mathrm{ord}_{p^{k+2}}(b) = p \cdot \mathrm{ord}_{p^{k+1}}(b)$. This type of argument can be continued indefinitely (formally, we could simply say that under the assumption (*) we showed that the exact same statement with $k + m$ replaced by $(k+m)+1$ was true, which is the inductive step for showing that (*) is true by induction! (We simply "called" $k + m$, k.) So we have proved (*) by induction. The initial step is literally the first part of our proof.). So (*) is true for all $m \geq 1$.

Applying this to $\mathrm{ord}_{p^2}(b) = p(p-1)$, we have that for every $k \geq 2$, $\mathrm{ord}_{p^k}(b) = p^{k-1}(p-1) = \Phi(p^k)$. So b is a primitive root modulo p^k .

The only place where this argument breaks down for the prime $p = 2$ is when we write $((p-1)/2)s^2 p^{k-1}$, since $(p-1)/2 = 1/2$ is not an integer. But we need to extract the initial p of $p((p-1)/2)s^2p^{k-1}$ from $p(p-1)/2$, rather than from p^{2k}, only when $k = 1$, otherwise $k \geq 2$ and we write this as $1 + p^{k+1}(s + p(\binom{p}{2} s^2 p^{k-2} + \binom{p}{3} s^3 p2k - 2 + \cdots$ instead. Then the proof goes through as before. And so, for $p = 2$, we have:

If $p = 2$, $k \geq 2$ and $\mathrm{ord}_{2^{k+1}}(b) > \mathrm{ord}_{2^k}(b)$, then $\mathrm{ord}_{2^{k+m}}(b) = 2^m \mathrm{ord}_{2^k}(b)$ for all $m \geq 1$.

So, for example, since $\mathrm{ord}_{16}(3) = 4 > 2 = \mathrm{ord}_8(3)$, we have $\mathrm{ord}_{2^k}(3) = 2^{k-2}$ for all $k \geq 3$. Since $(a, 8) = 1 \Rightarrow \mathrm{ord}_8(a) = 2 < 4 = \Phi(8)$, there is no no primitive root mod 2^k for $k \geq 3$; our proof above shows that $2^{k-2} < 2^{k-1} = \Phi(2^k)$ is the highest order possible.

Finally, with this result in hand, we can extend our result about n^{th} roots mod p:

Theorem: If p is an odd prime, $k \geq 1$, and $(a, p) = 1$, then the equation

$$x^n \equiv a \pmod{p^k} \text{ has } \begin{cases} (n, \Phi(p^k)) \text{ solutions}, & \text{if } a^{\frac{\Phi(p^k)}{(n,\Phi(p^k))}} \equiv 1 \\ 0 \text{ solutions}, & \text{if } a^{\frac{\Phi(p^k}{(n,\Phi(p^k))}} \equiv -1 \end{cases}$$