Finding kth Roots (Mod n)

Assuming that $\gcd(b, n) = \gcd(k, \phi(n)) = 1$, we can take advantage of the trick used in RSA encryption to find a value x that solves the congruence

$$x^k \equiv b \pmod{n}$$

Suppose $x = b^u$. If this were the case, then $x^k \equiv b \pmod{n}$ becomes

$$b^{ku} \equiv b \pmod{n}$$

Under the assumptions above (in particular, the one about $\gcd(b, n) = 1$), the above happens if and only if

$$b^{ku-1} \equiv 1 \pmod{n}$$

We know, however, by Euler's theorem that $b^{\phi(n)} \equiv 1 \pmod{n}$. Further, upon raising both sides to the c^{th} power for any integer c, we know

$$b^{c\phi(n)} \equiv 1 \pmod{n}$$

As such, we hunt for a u so that

$$ku - 1 = c\phi(n)$$

Equivalently, we solve

$$ku \equiv 1 \pmod{\phi(n)}$$

Solving this type of congruence is a routine process by now, so we skip the details -- other than to notice, solving this congruence does depend upon our assumption that $\gcd(k, \phi(n)) = 1$.

Finally, upon finding this value of u, we can compute $x = b^u$ (our solution) by successive squaring.

◆◆◆