We now continue with our study of solving polynomial congruences.

Thus far we have seen how to solve linear congruences of the form

$$ax \equiv b \pmod n$$

as well as how to use solutions of $f(x) \equiv 0 \pmod{p^n}$ to produce solutions of $f(x) \equiv 0 \pmod{p^{n+1}}$. Our next step is to study quadratic congruences of the form

$$(*) \qquad ax^2 + bx + c \equiv 0 \pmod p.$$

where p is an odd prime and $p \nmid a$.

Since $\gcd(p, 4a) = 1$, we have that equation $(*)$ is equivalent to equation

$$4a(ax^2 + bx + c) \equiv 0 \pmod p$$

However,

$$4a(ax^2+bx+c) = (2ax+b)^2 - (b^2-4ac)$$

we have that $(*)$ is equivalent to

$$(2ax+b)^2 \equiv (b^2-4ac) \pmod p.$$

Setting $y = 2ax+b$ and $d = b^2-4ac$, we see solving

$(*)$

$$y^2 \equiv d \pmod p.$$

(Check these are equivalent as an exercise!)

Note that we have reduced solving quadratic congruence down to solving congruences of the form

$$x^2 \equiv a \pmod{p}.$$

If $p \mid a$, then $x = 0$ is a solution. From now on we assume $p \nmid a$.

Let x_0 be a solution so that

$$x_0^2 \equiv a \pmod{p}.$$

Then we have $(x_0 - p)^2 = (p - x_0)^2 = p^2 - 2px_0 + x_0^2$

$$\equiv a \pmod{p}.$$

Thus, $p - x_0$ is another solution. If $x_0 \equiv p - x_0 \pmod{p}$, we have $2x_0 \equiv 0 \pmod{p} \Rightarrow p \mid x_0$. This contradicts $p \nmid a$, so there are two solutions. Thus, our congruence has exactly 2 solution or no solutions. (Your homework shows $f(x) \equiv 0 \pmod{p}$ has at most $\deg f$ solutions).

What we are really trying to do is determine all the perfect squares modulo p.

Def: Let p be an odd prime and $\gcd(a,p) = 1$. If $x^2 \equiv a \pmod{p}$ has a solution, then a is said to be a quadratic residue modulo p. Otherwise it is said to be a <u>quadratic nonresidue modulo</u> p.

<u>Example:</u> Consider $p=17$. To find the quadratic residues we can compute all the squares mod p. This is enough because if $a \equiv b \pmod{p}$, then $a^2 \equiv b^2 \pmod{p}$. So we are able to compute all quadratic residues by just looking at a complete residue system.

We have

$1^2 \equiv 1 \equiv 16^2 \pmod{17}$

$2^2 \equiv 4 \equiv 15^2 \pmod{17}$

$3^2 \equiv 9 \equiv 14^2 \pmod{17}$

$4^2 \equiv 16 \equiv 13^2 \pmod{17}$

$5^2 \equiv 8 \equiv 12^2 \pmod{17}$

$6^2 \equiv 2 \equiv 11^2 \pmod{17}$

$7^2 \equiv 15 \equiv 10^2 \pmod{17}$

$8^2 \equiv 13 \equiv 9^2 \pmod{17}$

Thus, the quadratic residues are $1, 2, 4, 8, 9, 13, 15, 16$ and the nonresidues are $3, 5, 6, 7, 10, 11, 12, 14$. Note that there are the same # of quadratic residues as nonresidues. Eventually we will prove this is true in general.

Before we can go into quadratic residues any further we need to develop the notion of primitive roots.

We know from Euler's theorem that any integer a w/ $\gcd(a,n)=1$ satisfies

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

However, it is often the case that there are smaller integers that we can raise a to and get 1 modulo 4. For example, we know that

$$\phi(16) = 8$$

but

$$15^2 \equiv 1 \pmod{16}.$$

This leads to the following definition:

<u>Def:</u> Let $n \in \mathbb{Z}_{>1}$ and $a \in \mathbb{Z}$ w/ $\gcd(a,n)=1$. The <u>order of a modulo n</u>, written $\mathrm{ord}_n(a)$, is the smallest positive integer so that $a^{\mathrm{ord}_n(a)} = 1 \pmod{n}$

Thus, in our example we had $\mathrm{ord}_{16}(15)=2$.

We only include $a \in \mathbb{Z}$ w/ $\gcd(a,n)=1$ since if $\gcd(a,n)=d>1$, we do not have a power we can raise a to and get 1. If we did, then $a(a^{\mathrm{ord}_n(a)-1}) \equiv 1 \pmod{n} \Rightarrow \gcd(a,n)=1$.

Thm: Let a have order $\mathrm{ord}_n(a)$ modulo n. Then $a^h \equiv 1 \pmod{n}$ iff $\mathrm{ord}_n(a) \mid h$. In particular, we see $\mathrm{ord}_n(a) \mid \phi(n)$.

Proof: "$\Rightarrow$" Let $\mathrm{ord}_n(a) = k$. Write $h = qk + r$ w/ $0 \le r < k$.

Then we have

$$\begin{aligned} 1 &\equiv a^h \pmod{n} \\ &\equiv a^{qk+r} \pmod{n} \\ &\equiv (a^k)^q a^r \pmod{n} \\ &\equiv a^r \pmod{n}. \end{aligned}$$

But this contradicts the minimality of k unless $r = 0$. Thus $q \mid h$.

"$\Leftarrow$" If $\mathrm{ord}_n(a) = k \mid h$, then $\exists\, t \in \mathbb{Z}$ w/ $h = tk$. Thus,

$$\begin{aligned} a^h &= a^{tk} \\ &= (a^k)^t \\ &\equiv 1^t \pmod{n} \\ &\equiv 1 \pmod{n} \end{aligned}$$

$\blacksquare$

This theorem significantly reduces our computations in looking for orders; we only need to look at those integers k that divide $\Phi(n)$!

Another basic fact is given by the following theorem.

Thm: Let $a \in \mathbb{Z}$ with $\mathrm{ord}_n(a) = k$. Then $a^i \equiv a^j \pmod{n}$ iff $i \equiv j \pmod{K}$.

Proof: "$\Rightarrow$" Suppose $a^i \equiv a^j \pmod{n}$. Then since $\gcd(a, n) = 1$, we can cancel out powers of a. WLOG assume that $i \ge j$.

Cancelling powers of a we obtain

$$a^{i-j} \equiv 1 \pmod n.$$

The previous theorem implies $k \mid i-j$, i.e., $i \equiv j \pmod n$.

"$\Leftarrow$" Suppose $i \equiv j \pmod k$. Write $i = j + kt$ for some $t \in \mathbb{Z}$.

Then we have

$$\begin{aligned} a^i &= a^{j+kt} \\ &= a^j (a^k)^t \\ &\equiv a^j (1)^t \pmod n \\ &\equiv a^j \pmod n \quad \blacksquare \end{aligned}$$

This theorem immediately shows that if $\operatorname{ord}_n(a) = k$, then $a, a^2, \ldots, a^k$ are all distinct modulo n. Note that if $\operatorname{ord}_n(a) = \phi(n)$, then we have $a, a^2, \ldots, a^{\phi(n)}$ are $\phi(n)$ distinct elements modulo n, so form a reduced residue system modulo n.

Thm: If $\operatorname{ord}_n(a) = k$ and $h \in \mathbb{Z}_{>0}$, then a^h has order $k/\gcd(h,k)$ modulo n.

Proof: We need to show that $a^{h\frac{k}{\gcd(h,k)}} \equiv 1 \pmod n$ and that $k/\gcd(h,k)$ is the smallest such integer.

Let $\operatorname{ord}_n(a^h) = r$. First observe that

$$\begin{aligned} (a^h)^{\frac{k}{\gcd(h,k)}} &= a^{\frac{hk}{\gcd(h,k)}} \\ &= (a^k)^{\frac{h}{\gcd(h,k)}} \equiv 1 \pmod n. \end{aligned}$$

We have necessarily that $r \mid \frac{k}{\gcd(h,k)}$. We also have that

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

$\Rightarrow k \mid hr$. Thus, $\frac{k}{\gcd(h,k)} \,\Big|\, \frac{hr}{\gcd(h,k)}$. Since $\gcd\left(\frac{h}{\gcd(h,k)}, \frac{k}{\gcd(h,k)}\right) = 1$, we must have $\frac{k}{\gcd(h,k)} \,\Big|\, r$.

Thus, $r = \frac{k}{\gcd(h,k)}$ as desired. □

Cor: Let $\mathrm{ord}_n(a) = k$. Then $\mathrm{ord}_n(a^h) = k$ iff $\gcd(k,h) = 1$.

Def: If $\gcd(a,n) = 1$ and $\mathrm{ord}_n(a) = \phi(n)$, we say a is a primitive root modulo n.

Note that in abstract algebra terms this says that a is a generator of $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e. $\langle a \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$.

The reason these primitive roots are important is exactly this fact. In our language, what this is saying is the following theorem.

Thm: Let $\gcd(a,n) = 1$ and let a be a primitive root. If $a_1, \dots, a_{\phi(n)}$ is a reduced residue system modulo n, then

$$\{a, a^2, \dots, a^{\phi(n)}\} \equiv \{a_1, a_2, \dots, a_{\phi(n)}\} \pmod{n}$$

in some order.

Proof: This fact is clear from the fact that the a^i are incongruent and the fact that the sets have the same number of elements. ∎

Corl: If there is a primitive root modulo n, then there are $\phi(\phi(n))$ of them.

Proof: Let a be a primitive root modulo n. Then $\{a, a^2, \ldots, a^{\phi(n)}\}$ give all the relatively prime elements modulo n. Thus, any other primitive root must be among these elements. An element a^h has order $\phi(n)$ iff $\gcd(h, \phi(n)) = 1$ since the order of a^h is given by

$$\phi(n) / \gcd(h, \operatorname{ord}_a(n)) = \phi(n) / \gcd(h, \phi(n))$$

$$= \phi(n) \quad \text{iff} \quad \gcd(h, \phi(n)) = 1.$$

There are precisely $\phi(\phi(n))$ integers $1 \leq h \leq \phi(n)$ that are relatively prime to $\phi(n)$. ∎

Here is an easy way to find primitive roots modulo n.

(There are probably much better ways, but I was having issues with the commands in SAGE that are preprogrammed!)

```
R = Integers(n).     (this constructs Z/nZ).
for i in range (0,n):
    if gcd(i,n)==1:
        ~~print~~
        if R(i).multiplicative_order() = euler_phi(n):
            print(i)
```

For example, if we run this with $n=10$ it returns 3, 7. Thus, 3 and 7 are primitive roots modulo 10.

If we run this with $n=726$, it returns nothing letting us know there are no primitive roots modulo 726.

This naturally leads to the question of for which n do primitive roots exist?

We begin by showing that if $n=p$ a prime then there is a primitive root modulo p. In terms of abstract algebra, this is just the statement that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. This takes some effort to prove even with abstract algebra.

In the homework you will prove the following theorem:

Thm (Lagrange): If p is prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

with $a_n \not\equiv 0 \pmod{p}$, then $f(x) \equiv 0 \pmod{p}$ has at most n distinct solutions modulo p.

Recall that if the modulus isn't prime this statement is not necessarily true! For example, $f(x) = x^2 - 1$ has 4 distinct solutions modulo 15!

Cor: If p is a prime and $d \mid p-1$, then

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Note that this does not give us the existence of primitive roots. It could be that all the solutions have order less than $p-1$ as far as this theorem tells us!

Proof: We use the fact that $d \mid (p-1)$ to conclude $\exists\, t \in \mathbb{Z}$ s.t $p-1 = dt$. Thus, $\exists\, f(x) \in \mathbb{Z}[x]$ so that

$$x^{p-1} - 1 = (x^d - 1) f(x).$$

In particular, one can calculate that

$$f(x) = x^{d(t-1)} + x^{d(t-2)} + \dots + x^d + 1.$$

Lagrange's theorem gives that

$$f(x) \equiv 0 \pmod{p}$$

has at most $dt - d = p-1-d$ solutions. Fermat's little theorem gives that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p-1$ incongruent solutions modulo p.

We claim that any solution of

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

that is not a solution of

$$f(x) \equiv 0 \pmod{p}$$

must satisfy the congruence

$$x^{d} - 1 \equiv 0 \pmod{p}.$$

This follows immediately from the factorization of $x^{p-1} - 1$ and the fact that p is prime. Thus,

$$x^{d} - 1 \equiv 0 \pmod{p}$$

must have at least

$$(p-1) - (p-1-d) = d$$

incongruent solutions modulo p. Since Lagrange's thm says it can have at most d, we have the result. ▨

We need the following theorem of Gauss:

<u>Thm:</u> For each $n \in \mathbb{Z}_{\geq 1}$,

$$n = \sum_{d \mid n} \phi(d).$$

<u>Proof:</u> We separate the integers k w/ $1 \leq k \leq n$ by setting

$$S_d = \{ m : \gcd(m,n) = d, \ 1 \leq m \leq n \}.$$

We have shown that $\gcd(m,n) = d$ iff $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

This gives that S_d contains integers relatively prime to $\frac{n}{d}$ that do not exceed n/d. This is precisely $\phi(n/d)$,

Since each integer lies in some S_d, we have

$$n = \sum_{d \mid n} \# S_d = \sum_{d \mid n} \phi\left(\frac{n}{d}\right)$$

$$= \sum_{e \mid n} \phi(e). \quad \blacksquare$$

We will use this theorem to prove the following result:

<u>Thm:</u> Let p be a prime and $d \in \mathbb{Z}_{\geq 1}$ s.t. $d \mid p-1$. There are $\phi(d)$ distinct numbers modulo p w/ $\text{ord}_p = d$,

Proof: Let $\psi(d)$ be the number of integers k w/ $1 \le k \le p-1$ and $\text{ord}_p(k) = d$. Each k w/ $1 \le k \le p-1$ must have order $e \mid p-1$ for some e since $\phi(p) = p-1$. Thus,

$$p-1 = \sum_{d \mid p-1} \psi(d).$$

We also know that

$$p-1 = \sum_{d \mid p-1} \phi(d).$$

and so

$$\sum_{d \mid p-1} \phi(d) = \sum_{d \mid p-1} \psi(d).$$

If we can show that $\psi(d) \le \phi(d)$ $\forall$ $d \mid p-1$, we will have $\psi(d) = \phi(d)$ as desired since then

$$\sum_{d \mid p-1} \psi(d) \le \sum_{d \mid p-1} \phi(d) = \sum_{d \mid p-1} \psi(d)$$

$\Rightarrow$ $\le$ must be $=$.

Let $e \mid p-1$. Either $\psi(e) = 0$ or $\psi(e) > 0$. If $\psi(e) = 0$, then trivially we have $\psi(e) \le \phi(e)$. Thus, assume $\psi(e) > 0$; i.e, $\exists$ a w/ $1 \le a \le p-1$ and $\text{ord}_p(a) = e$. Thus we have e distinct integers $a, a^2, .., a^e$ all zeros of

$$x^e - 1 \equiv 0 \pmod p.$$

But we have shown these are all the solutions to this congruence. Thus, any integer of order ~~d~~ e must be congruent to one of these. However, among the a^k's there are only $\phi(e)$ w/ order e, namely the ones w/ $\gcd(k,e)=1$. $\Rightarrow \psi(e)=\phi(d)$.

Thus we have the result. $\blacksquare$

This theorem shows that there are always primitive root modulo p since $p-1 \mid p-1$.

Before we return to quadratic congruences, we prove a couple of interesting results concerning primitive roots. We will determine exactly when an integer n has a primitive root.

<u>Thm:</u> If $\gcd(m,n)>1$ and $m,n>2$, then there are no primitive roots modulo mn.

<u>Proof:</u> We claim that the order of any integer a w/ $\gcd(a,mn)=1$ is less than or equal to $\frac{\phi(mn)}{2}$. If we show this, then clearly there are no primitive roots modulo mn.

Since m and n are both greater than 2, each has an odd prime that divides it. Thus, if $p \mid m$, p odd, then $p-1 \mid \phi(m)$ and so $\phi(m)$ is even. Similarly we get $\phi(n)$ is even. Thus, $\gcd(\phi(m),\phi(n)) \geq 2$.

We have if $d = \gcd(\phi(m), \phi(n))$,

$$h = \text{lcm}(\phi(m), \phi(n)) = \frac{\phi(m)\phi(n)}{d} \le \frac{\phi(m)\phi(n)}{2}.$$

By Euler we know

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

$\Rightarrow$

$$\phi \quad \left(a^{\phi(m)}\right)^{\frac{\phi(n)}{d}} \equiv 1 \pmod{m}$$

$\Rightarrow$

$$a^h \equiv 1 \pmod{m}.$$

Similarly we get $a^h \equiv 1 \pmod{n}$. Since $\gcd(m,n) = 1$, we have

$$a^h \equiv 1 \pmod{mn}, \quad \text{i.e., } \text{ord}_{mn}(a) \le h \le \frac{\phi(m)\phi(n)}{2}. \quad \blacksquare$$

The next step is to investigate powers of 2.

Thm: For $k \ge 3$, there are no primitive roots modulo 2^k.

Proof: We claim that for any odd integer a, if $k \ge 3$ then (*) $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Granting this claim for a moment, lets see how to finish the proof.

The integers relatively prime to $\phi(2^k)$ are the odd integers less then 2^k, which ~~there~~ there are 2^{k-1} of, i.e., $\phi(2^k) = 2^{k-1}$.

However, given the claim we know $\text{ord}_{2^k}(a) \le 2^{k-2} = \phi(2^k)/2$

for all odd a, Thus there are no primitive roots. So it only remains to prove (*) to finish the proof. We prove this by induction on k.

$k = 3$:

$$a^2 \equiv 1 \pmod 8 ?$$

Just check the cases $1^2, 3^3, 5^2, 7^2 \equiv 1 \pmod 8$.

Now assume the statement is true for all $3 \le n \le N$ for some $N \in \mathbb{Z}_{\geq 3}$. In particular,

$$a^{2^{N-2}} \equiv 1 \pmod{2^N}.$$

So $\exists\ t \in \mathbb{Z}$ s.t

$$a^{2^{N-2}} = 1 + t2^N.$$

If we square both side we obtain

$$\begin{aligned} a^{2^{N-1}} &= 1 + 2^{N+1}t + t^2 2^{2N} \\ &= 1 + 2^{N+1}(t + t^2 2^{N-1}) \\ &\equiv 1 \pmod{2^{N+1}}, \end{aligned}$$

as desired. Thus (*) holds for all $k \geq 3$ by induction. ∎

We combine these results to conclude:

Cor: If n is divisible by 2 odd primes or $n = 2^m p^k$ where p is odd prime, $m \geq 2$ then there are no primitive root modulo n.

Proof: This corollary is just special cases of the theorem above with $\gcd(m,n)=2$. ■

Thus, we only have to consider

$$n = 2,\ 4,\ p^k,\ \text{and } 2p^k$$

where p is an odd prime as possibilities for having primitive roots! The positive is that we will have a complete classification of when n has a primitive root. The negative is that most n's do not have primitive roots and primitive roots ~~appear~~ often make life much easier!

We now must prove some rather painful technical lemmas to prepare us to prove our main result.

Lemma: Let p be an odd prime. There exists a primitive root r of p such that

$$r^{p-1} \not\equiv 1 \pmod{p^2}.$$

Proof: We already know there are primitive roots modulo p, so choose one and call it r. If we have that

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

we are done. Assume $r^{p-1} \equiv 1 \pmod{p^2}$. Then we have

$$(r+p)^{p-1} = r^{p-1} + (p-1)pr^{p-2} + \cdots$$
$$\equiv r^{p-1} \pmod{p}$$
$$\equiv 1 \pmod{p}.$$

There are no smaller powers clearly, so $r+p$ is also a primitive root modulo p. (they are equal modulo p, duh...) Looking modulo p^2 we have:

$$(r+p)^{p-1} = r^{p-1} + (p-1)pr^{p-2} + \binom{p-1}{2}p^2r^{p-3} + \cdots$$
$$\equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}$$

We assumed $r^{p-1} \equiv 1 \pmod{p^2}$, so

$$(r+p)^{p-1} \equiv 1 + (p-1)pr^{p-2} .$$

Since r is primitive modulo p, $p \nmid r$. $\Rightarrow p \nmid r^{p-2}$. $\Rightarrow$

$$(r+p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

So we have the result. ■

Cor: Let p be an odd prime. There is a primitive root modulo p^2. More precisely, if r is a primitive root modulo p, either r or $r+p$ is a primitive root modulo p^2.

Proof: Observe that $\phi(p^2) = p(p-1)$, so if r is primitive mod p, Then r has order $p-1$ or $p(p-1)$ modulo p^2. (It must divide

$\phi(p^2)$, and if we had $r^p \equiv 1 \pmod{p^2}$, then $r^p \equiv 1 \pmod{p}$

$\Rightarrow$ $r(r^{p-1}) \equiv 1 \pmod{p}$ $\Rightarrow$ $r \equiv 1 \pmod{p}$!) If r has order $\phi(p)$ modulo p^2 we are done. If r has order $p-1$ modulo p^2, then we just saw that $r+p$ must have order $\phi(p)$. (It can't have order $p-1$ from last proof!). ■

Lemma: Let p be an odd prime and r a primitive root modulo p so that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each $k \in \mathbb{Z}_{\geq 2}$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Proof: We prove this by induction on k. The case $k=2$ was our previous lemma. Suppose the result holds for $2 \leq n \leq N$ for some $N \in \mathbb{Z}_{\geq 2}$. Since r is primitive modulo p, $\gcd(r, p) = 1$ so Euler $\Rightarrow$

$$r^{\phi(p^{N-1})} = 1 \pmod{p^{N-1}}$$

i.e.,

$$r^{p^{N-2}(p-1)} \equiv 1 \pmod{p^{N-1}}.$$

So $\exists$ $t \in \mathbb{Z}$ s.t.

$$r^{p^{N-2}(p-1)} = 1 + tp^{N-1}.$$

w/ $p \nmid t$ (by induction hyp).

Raising both sides to the p we get:

$$r^{p^{N-1}(p-1)} = (1+tp^{N-1})^p$$

$$\equiv 1 + tp^N \pmod{p^{N+1}}$$

However, since $p \nmid t$, this gives that

$$r^{p^{N-1}(p-1)} \not\equiv 1 \pmod{p^{N+1}}$$

as desired. ■

We are now able to prove the following theorem.

Thm: Let p be an odd prime and let $k \in \mathbb{Z}_{\geq 1}$. There exists a primitive root modulo p^k.

Proof: Choose r a primitive root so that

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Let $n = \operatorname{ord}_{p^k}(r)$. We know $n \mid \phi(p^k) = p^{k-1}(p-1)$. Using the fact that $r^n \equiv 1 \pmod{p^k}$, we also have $r^n \equiv 1 \pmod{p} \to n \mid p-1$ as well. Thus, we can write $n = p^m(p-1)$ for some $0 \leq m \leq k-1$. If $n \neq p^{k-1}(p-1)$, then we would have $n \mid p^{k-2}(p-1)$ and so

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}. \qquad \#.$$

Thus $n = p^{k-1}(p-1)$ and r is a primitive root modulo p^k. □

Finally, we deal with the case of $n = 2p^k$.

<u>Cor:</u> There are primitive roots modulo $2p^k$ for p an odd prime and $k \geq 1$.

<u>Proof:</u> Let r be a primitive root modulo p^k. We may assume r is odd. (if not, $r + p^k$ is odd and still a primitive root modulo p^k!) So $\gcd(r, 2p^k) = 1$. The $\overset{n}{\frown}$order of r modulo $2p^k$ must divide

$$\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k).$$

However,

$$r^n \equiv 1 \pmod{2p^k} \Rightarrow r^n \equiv 1 \pmod{p^k}$$

$\Rightarrow$ And $\phi(p^k) \mid n$. Thus, $\phi(p^k) = n$. □

We will now use this theory to study quadratic congruences further. We sum up with the following theorem.

Thm: Let $n \in \mathbb{Z}_{>1}$. There is a primitive root modulo n iff

$$n = 2, 4, p^k, 2p^k$$

for p an odd prime.