We have focused on solving congruence equations, e.g.

$x^n \equiv_p a$ $\quad x^n - a \equiv_p 0$ for prime modulus.

But what about other moduli? $x^n - a \equiv_N 0$?

What can we say? Plenty!

Thm: If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, and N, M integers with $(N,M) = 1$, and $f(x) \equiv_N 0$, $f(x) \equiv_M 0$ both have a solution, then so does $f(x) \equiv_{NM} 0$.

Pf: Suppose $f(a) \equiv_N 0$, $f(b) \equiv_M 0$. We know that if $c \equiv_N a$, then $f(c) \equiv_N f(a) \equiv_N 0$, so c is also a solution. We also know that $f(c) \equiv_N 0$ and $f(c) \equiv_M 0 \Rightarrow$ $N \mid f(c)$, $M \mid f(c)$ so $NM \mid f(c)$ so $f(c) \equiv_{NM} 0$. So it is enough to show that there is a c with

$c \equiv_N a$ and $c \equiv_M b$, i.e. there is a simultaneous solution to the system of eqns

$x \equiv a \pmod N$
$x \equiv b \pmod M$

But this is the Chinese Remainder Thm!

Quick proof of CRT: (*) $x = a + Nk$, $x = b + Ml$, & want

$a + Nk = b + Ml$ some k, l i.e. $b - a = Ml - Nk$

But $(M,N) = 1 \Rightarrow 1 = Ml_0 - Nk_0$ some l_0, k_0 so

$b - a = M(b-a)l_0 - N(b-a)k_0$, so set $x = a + N(\#(b-a)k_0)$

Check: any other solution x' of (*) has $x \equiv x' \pmod{MN}$

So for every possible pair of solutions $f(a) \underset{N}{\equiv} 0$, $f(b) \underset{M}{\equiv} 0$ (mod N, M resp.), there is exactly one solution ν to

$f(\nu) \underset{MN}{\equiv} 0 \pmod{MN}$

~~# of incongruent (mod MN) solns to $f(x) \underset{MN}{\equiv} 0$~~

So if we call $s(N) =$ # of incongruent solutions (mod N) to $f(x) \underset{N}{\equiv} 0$, we in fact have

$$\boxed{s(NM) = s(N)s(M)}$$

~~So for~~ More generally, if $N = n_1 \cdots n_k$ with $(n_i, n_j) = 1$ ~~for~~ for $i \neq j$ then

$s(N) = s(n_1) \cdots s(n_k)$ (by induction!)

So to decide if $f(x) \underset{N}{\equiv} 0$ has any solutions, it is enough, writing $N = p_1^{r_1} \cdots p_k^{r_k}$ $p_1 < \cdots < p_k$ prime, if

$f(x) \underset{p_i^{r_i}}{\equiv} 0$ for each i.

We showed: For p prime, deciding if

$x^r \underset{p}{\equiv} a$ has a solution is straightforward.

check if $a^{\frac{p-1}{(r,p-1)}} \underset{p}{\equiv} 1$. Yes → $(r,p-1)$ solutions
No → no solution

But it wasn't really important that p be prime! Only that there is a primitive root of 1 mod p (and its order is $p-1$.) More generally:

(so a and a solution x was a power of it)

If there is a primitive root of 1 mod N, then

$x^r \underset{N}{\equiv} a$ has a solution (for $(a,N)=1$) $\Longleftrightarrow$

$a^{\frac{\phi(N)}{(\phi(N),r)}} \underset{N}{\equiv} 1$ our proof goes straight through!

I should have stated that

There is a primitive root of 1 mod n $\Longleftrightarrow$
n = one of $2, 4, p^k, 2p^k$ & p = odd prime.

Combining with the previous result, deciding if

$x^r \underset{N}{\equiv} a$ has any solution (and how many!) boils down to deciding if $x^r \underset{p_i^{r_i}}{\equiv} a$ has solutions, which for p_i odd is straightforward; for $p=2$ it is a little trickier!

Why is there a primitive root of 1 mod p^2 for p odd and prime?

There is a primitive root mod p, call it a. Then

Claim: $a+tp$ $0 \le t \le p-1$ is a prim root mod p^2 for all but one value of t.

$k_t = \text{ord}_{p^2}(a+tp)$

$(a+tp)^{k_t} \underset{p^2}{\equiv} 1 \Longrightarrow (a+tp)^{k_t} \underset{p}{\equiv} a^{k_t} \underset{p}{\equiv} 1$ so $p-1 \mid k_t$

since $\phi(p^2) = p(p-1)$ so $k_t \mid p(p-1)$ either $k_t = p-1$ or $k_t = p(p-1)$.

If $k_t = p(p-1)$ then $a+tp$ is a primitive root.

So we want to show that $k_t = p-1$ for only one value of t.

I.e., if $(a+tp)^{p-1} \underset{p^2}{\equiv} 1$ then $(a+t'p)^{p-1} \underset{p^2}{\not\equiv} 1$ for $t' \not\equiv_p t$

But! $(a+t'p)^{p-1} = ((a+tp)+np)^{p-1}$ $\boxed{n \not\equiv_p 0}$

$= (a+tp)^{p-1} + (p-1)(a+tp)^{p-2}(np) + \binom{p-1}{2}(a+tp)^{p-2}(np)^2$

$+ \cdots$

$\underset{p^2}{\equiv} 1 + (p-1)(a+tp)^{p-2}(np) + 0 + 0 \cdots + 0$

$\underset{p^2}{\equiv} 1 + [(p-1)(a+tp)^{p-2}n]p \underset{p^2}{\not\equiv} 1$!

$\not\equiv_p 0$

& each primitive root mod p ($\phi(p-1)$ of them)
give $(p-1)$ distinct prim roots mod p^2
$\Rightarrow$ there are $(p-1)\phi(p-1) = \phi(\phi(p^2))$ prim roots mod p^2.

Thm
If a is a prim root mod p^2 for p = odd prime,
then a is a prime root mod p^r for all $r \geq 2$.

By induction: $r=2$ ✓ Assume true for $r-1$

$n = \text{ord}_{p^r}(a)$ then $a^n \equiv_{p^r} 1 \Rightarrow a^n \equiv_{p^2} 1 \Rightarrow p(p-1) \mid n$;
and $n \mid \phi(p^r) = p^{r-1}(p-1)$, & $n = p^\beta(p-1)$ for some $1 \leq \beta \leq r-1$.

Claim: $\beta = r-1$. Proof: show $a^{p^{r-2}(p-1)} \not\equiv_{p^r} 1$

we know that $\text{ord}_{p^{r-1}}(a) = \phi(p^{r-1}) = p^{r-2}(p-1)$, and
$\text{ord}_{p^{r-2}}(a) = p^{r-3}(p-1)$ so $a^{p^{r-3}(p-1)} \equiv_{p^{r-2}} 1$ but $\not\equiv_{p^{r-1}} 1$

& $a^{p^{r-3}(p-1)} = 1 + sp^{r-2}$ with $p \nmid s$. then

$$a^{p^{r-2}(p-1)} = (a^{\cdots})^p = (1+sp^{r-2})^p = 1^p + p\,sp^{r-2} + \text{high powers of } p \geq r$$
$$\equiv_{p^r} 1 + sp^{r-1} \not\equiv_{p^r} 1 \quad \text{since } p \nmid s. \quad \blacksquare$$