NT Notes 5

$$\left.\begin{array}{l}\varphi(p^k) = p^{k-1}(p-1) \\ \varphi(m \cdot n) = \varphi(m)\varphi(n) \\ \quad \text{for } \gcd(m,n) = 1\end{array}\right\}$$

~~(Try without brute force)~~

1 Find the incongruent roots modulo 11 of

(i) $x^2+2 = x^2-9$
$= (x-3)(x+3)$
$\quad 3 \qquad 8$

(ii) x^4+x^2+1
None b/c you only need to check $\{0, \ldots, 5\}$ (even)
Also $2x^2 = -1 \pm 2\sqrt{2}$ and 2 is not square.

3 ~~2~~. Find the [illegible] primitive roots of 13 up to congruence

? $\overset{2}{\cancel{1}}, \overset{6}{\cancel{5}}, 7, 11$ Also $\varphi(12) = \varphi(3)\varphi(2^2) = 4$

2 ~~3~~. How many primitive roots does 109 have?

Note (1) 109 is prime and (2) $\varphi(108) = \varphi(2^2)\varphi(3^3) = 2(2-1)3^2(3-1)$ $= 2 \cdot 9 \cdot 2 = 36$

Really say "prove 2 is a primitive root of 13. What are the others $2^1 \equiv 2 \quad 2^5 \equiv 6 \quad 2^7 \equiv 11 \quad 2^{11} \equiv 7$.

4*. For a primitive root g of p (prime), prove that $-g$ is a primitive root iff $p \equiv 1 \pmod 4$.

$(\Leftarrow)$ $g^{p-1} \equiv_p 1 \Rightarrow g^{4k} \equiv_p 1 \Rightarrow (g^{2k})^2 \equiv_p 1 \Rightarrow \begin{cases} \cancel{g^{2k} \equiv_p 1} & \text{b/c } g \text{ primitive so } p-1 \text{ minimal} \\ g^{2k} \equiv_p -1 \longrightarrow (-g)^{2k} \equiv -1 \Rightarrow -g^{2k+1} \equiv_p g \end{cases}$ (primitive)

* Find all n for which $n!+9$ is a perfect cube (HINT: no Wilson)

If $27 \mid n!$ then $9 \mid (n!+9)$ but $27 \nmid (n!+9)$, so it cannot be a cube. So $n < 9$, and $n = 6$ is it.

* Find all ordered pairs $(p\ q)$ of primes such that $pq \mid p^q + q^p + 1$.

HINT: Fermat's little theorem. (*) $a^{p-1} \equiv_p 1$

Note $pq \mid p^q + q^p + 1 \Rightarrow p \mid q^p + 1 \overset{(*)}{\Rightarrow} p \mid q+1$. Symmetrically $q \mid p+1$. If both p and q are odd primes, $p+1$ and $q+1$ are even, so $2p \mid q+1$ and $2q \mid p+1$, so $p \le \frac{q+1}{2}$ $q \le \frac{p+1}{2}$, which by adding them tells us $p+q \le 2$ ↯ Wlog $p=2$, and $q \mid 3$.