Handout (Sections 8.1 & 8.2)

① We know that $ord_n(a) \mid \phi(n)$
But for any d divisor of $\phi(n)$, it is not always true that there exists an integer a with $ord_n(a) = d$. e.g. $n=12$, $\phi(12)=4$ but there is no integer of order 4 modulo 12;
$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12},$$ so all a coprime to n have orders 1 or 2.
(Looking ahead, this shows $n=12$ has no primitive roots).

② If we know one primitive root, say a, of n, then we can easily find all the other primitive roots of n: Set of primitive roots of $n = \{a^k : \gcd(k,\phi(n))=1\}$, $1 \le k \le \phi(n)$

③ Read Example 8.2

④ $ord_{23}(3) = ?$ $ord_{23}(5) = ?$
Since $\phi(23) = 22 = 2 \cdot 11$ we only have to consider the following powers of 3 & 5
$3^1 \equiv 3$, $3^2 \equiv 9$, $3^{11} \equiv 1 \pmod{23} \Rightarrow ord_{23}(3) = 11$
$5^1 \equiv 5$, $5^2 \equiv 2$, $5^{11} \equiv 22$, $5^{22} \equiv 1 \pmod{23} \Rightarrow ord_{23}(5) = 22$

⑤ If $ord_n(a) = n-1$ then n is prime.
Pf. By Thm., $n-1 \mid \phi(n)$. Since $\phi(n) \le n$, this means $\phi(n) = n-1$ which is possible iff n is prime

⑥ The odd prime divisors of the integer n^4+1 are of the form $8k+1$.
Pf. $p \mid n^4+1 \Rightarrow n^4 \equiv -1 \pmod p \Rightarrow n^8 \equiv 1 \pmod p$. By Thm 8.1, $ord_p(n) \mid 8$
But • $n^1 \equiv 1 \pmod p$ would mean $n^4+1 \equiv 2 \pmod p$ & $2 \not\equiv 0 \pmod p$ since p is odd.
• $n^2 \equiv 1 \pmod p$ would mean $n^4 \equiv 1 \pmod p$ & $1 \not\equiv -1 \pmod p$ since p is odd.
• We know $n^4 \equiv -1 \pmod p$ & $-1 \not\equiv 1 \pmod p$. Hence, $ord_p(n) = 8$
By Thm. 8.1, $8 \mid \phi(p)$ i.e., $8 \mid p-1$ i.e, $p = 8k+1$.

(7) There are infinitely many primes of the form $8k+1$.

Pf. Assume there are only finitely many primes of form $8k+1$, say $q_1, \ldots, q_r$.

Consider $N = (2q_1 \cdots q_r)^4 + 1$

$N > 2$ and odd. So, it has only odd prime factors, which by (6) are all of the form $8k+1$.

Say p is an odd prime of N, then $p = q_i$ for some i.

$\therefore$ $p \mid N$ & $p \mid (2q_1 \cdots q_r)^4$

This implies $p \mid N - (2q_1 \cdots q_r)^4 = 1$ contradiction.

(8) 12 has no primitive roots (see (1)).

(9) 2 is primitive root of 19 but not of 17. [Recall $\phi(19)=18$ & $\phi(17)=16$

Soln. Modulo 19, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 7$, $2^9 \equiv 18 \equiv -1$, $2^{18} \equiv 1$

Thus 2 is a primitive root of 19

Modulo 17, $2^2 \equiv 4$, $2^4 \equiv 16 \equiv -1$, $2^8 \equiv 1$.

Thus, $ord_{17}(2) = 8 \neq 16 = \phi(17)$.

(10) Let r be a primitive root of n. Then,

r^k is a primitive root of $n \Leftrightarrow \gcd(k, \phi(n)) = 1$

Pf. By Thm 8.3, $ord_n(r^k) = \dfrac{\phi(n)}{\gcd(k, \phi(n))}$

Thus, r^k is a primitive root of $n \Leftrightarrow ord_n(r^k) = \phi(n)$

$\Leftrightarrow \gcd(k, \phi(n)) = 1$.

(11) $x^2 - 1 \equiv 0 \pmod{15}$ has four incongruent solutions modulo 15, namely $x \equiv 1, 4, 11, \& 14 \pmod{15}$ showing that Lagrange's Thm. need not hold when the modulus is not a prime.

(12) The only incongruent solns of $x^2 - 1 \equiv 0 \pmod p$ are 1 & $p-1$

Soln. $1^2 \equiv (p-1)^2 \equiv 1 \pmod p$. Thus, $x^2 - 1 \equiv 0 \pmod p$ has two incongruent solutions & By Lagrange's Thm., it cannot have any more solutions.