Handout (Sections 8.1 & 8.2)

1. We know that \( \text{ord}_n(a) \mid \phi(n) \)
   But for any \( d \) divisor of \( \phi(n) \), it is not always true that there exists an integer \( a \) with \( \text{ord}_n(a) = d \). 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 \( a \), \( a \equiv n \), then we can easily find all the other primitive roots of \( a \) \( \pmod{n} \). Set \( g \) primitive roots \( \pmod{n} \) \( n = 2^k \cdot \ell \) \( \gcd(k,\phi(n)) = 1 \) \( 1 \leq k \leq \phi(n) \)

3. Read Example 8.2

4. \( \text{ord}_{23}(3) = ? \), \( \text{ord}_{23}(5) = ? \)
   Since \( \phi(23) = 22 = 2 \cdot 11 \), we only have to consider the following powers of 3 \& 5:
   \[ 3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 1 \pmod{23} \Rightarrow \text{ord}_{23}(3) = 11, \]
   \[ 5^1 \equiv 5, \quad 5^2 \equiv 2, \quad 5^3 \equiv 22, \quad 5^{22} \equiv 1 \pmod{23} \Rightarrow \text{ord}_{23}(5) = 22 \]

5. If \( \text{ord}_n(a) = n-1 \) then \( n \) is prime.
   By Thm., \( n-1 \mid \phi(n) \). Since \( \phi(n) \leq n \), this means \( \phi(n) = n-1 \)
   Which is possible iff \( n \) is prime.

6. The odd prime divisors of the integers \( n^4+1 \) are of the form \( 8k + 1 \).
   If \( p \mid n^4+1 \Rightarrow n^4 \equiv -1 \pmod{p} \Rightarrow n^8 \equiv 1 \pmod{p} \). By Thm 8.1, \( \text{ord}_p(n) \mid 8 \)
   But \( n^8 \equiv 1 \pmod{p} \) would mean \( n^4 \equiv 2 \pmod{p} \) \& \( 2 \not\equiv 0 \pmod{p} \) since \( p \) is odd.
   * \( n^8 \equiv 1 \pmod{p} \) would mean \( n^4 \equiv 1 \pmod{p} \) \& \( 1 \not\equiv -1 \pmod{p} \). Hence, \( \text{ord}_p(n) = 8 \)
   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 \(8k+1\).

8. Assume there are only finitely many primes of the form \(8k+1\), say \(q_1, \ldots, q_m\).

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

\(N \geq 2\) 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 \(i\).

\(\therefore p \mid N \land p \mid (2q_1 \cdots q_m)^4\)

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

8. 12 has no primitive roots (see 6).

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

\(\text{Modulo 19}, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^6 \equiv 7, \quad 2^9 \equiv 18 \equiv -1, \quad 2^{18} \equiv 1\)

Thus, 2 is a primitive root of 19

\(\text{Modulo 17}, \quad 2^2 \equiv 4, \quad 2^4 \equiv 16 \equiv -1, \quad 2^8 \equiv 1\)

Thus, \(\text{ord}_n(2) = 8 \neq 16 = \phi(17)\).

10. Let \(x\) be a primitive root of \(\phi(n)\). Then

\(x^k\) is a primitive root of \(n \iff \gcd(k, \phi(n)) = 1\)

\(\therefore \text{By Thm 8.3, ord}_n(x^k) = \phi(n) = \frac{\gcd(k, \phi(n))}{\gcd(k, \phi(n))}\)

Thus, \(x^k\) is a primitive root of \(n \iff \text{ord}_n(x^k) = \phi(n) \iff \gcd(k, \phi(n)) = 1\).

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 solutions of \(x^2 - 1 \equiv 0 \pmod{p}\) are 1 & \(p - 1\).

\(\text{Thus, } 4^2 \equiv (p - 1)^2 \equiv 1 \pmod{p}. \text{ Thus, } x^2 - 1 \equiv 0 \pmod{p} \) has two incongruent solutions. By Lagrange's Thm, it cannot have any more solutions.