1. Show that 91 is a Fermat Pseudoprime to the base 3. Note that 91 is not prime!

**Solution:**
Show that $3^{90} \equiv 1 \mod 91$.

2. Prove that if $n \geq 2$ and $\gcd(6, n) = 1$ then $\phi(3n) = 2\phi(2n)$.

**Solution:**
Since $\gcd(6, n) = 1$ we know $\gcd(2, n) = \gcd(3, n) = 1$ and then we have $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$ and $2\phi(2n) = 2\phi(2)\phi(n) = 2\phi(n)$.

3. Classify all numbers $n$ for which $\tau(n) = 12$.

**Solution:**
If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1) = 12$. The ways to get a product of 12 are $(12) = (2)(6) = (3)(4) = (2)(2)(3)$ so we can have at most three primes and so either $n = p^{11}$, $n = pq^3$, $n = p^2q^2$, or $n = pq^2$.

4. Suppose $n$ is a perfect number and $p$ is a prime such that $pn$ is also perfect. Prove $\gcd(p, n) \neq 1$.

**Solution:**
By contradiction. If $\gcd(p, n) = 1$ then $2pn = \sigma(pn) = \sigma(p)\sigma(n) = \sigma(p)(2n)$ so $\sigma(p) = p$ which is a contradiction since $\sigma(p) = p + 1$.

5. Prove that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod ab$ if $\gcd(a, b) = 1$.

**Solution:**
Since $\gcd(a, b) = 1$ we have $a^{\phi(b)} \equiv 1 \mod b$. Then since $b \equiv 0 \mod b$ we get $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod b$.

Since $\gcd(a, b) = 1$ we have $b^{\phi(a)} \equiv 1 \mod a$. Then since $a \equiv 0 \mod a$ we get $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod a$.

Since $\gcd(a, b) = 1$ we then get $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod ab$.

6. Suppose that $p$ is prime and $n \in \mathbb{Z}^+$. Prove that $p \nmid n$ iff $\phi(pm) = (p - 1)\phi(n)$.

**Solution:**
Suppose $p \nmid n$ then $\gcd(p, n) = 1$. Then $\phi(pm) = \phi(p)\phi(n) = (p - 1)\phi(n)$.

On the other hand if $p \mid n$ then $n = p^\alpha N$ where $\gcd(p, N) = 1$ (factoring out all the $p$) and so

$$\phi(pm) = \phi(pp^\alpha N) = \phi(p^{\alpha+1}N) = \phi(p^{\alpha+1})\phi(N) = (p^{\alpha+1} - p^\alpha)\phi(N)$$

$$= p(p^\alpha - p^{\alpha-1})\phi(N) = p\phi(p^\alpha)\phi(N) = p\phi(p^\alpha N) = p\phi(n) \neq (p - 1)\phi(n)$$

7. (a) Show that 3 is a primitive root modulo 17.

**Solution:**
Just show that $\text{ord}_{17} 3 = \phi(17) = 16$. 
(b) Find all primitive roots modulo 17.

**Solution:**
These will be $3^k$ for all $k$ with $\gcd(k, \phi(17)) = 1$.

8. A partial table of indices for 7, a primitive root of 13 is given here:

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>ind$_7a$</td>
<td>12</td>
<td>b</td>
<td>8</td>
<td>10</td>
<td>3</td>
<td>7</td>
<td>a</td>
<td>9</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

(a) Find $a$ and $b$.

**Solution:**
We have $\text{ind}_7 7 = 1$ because $7^1 \equiv 7 \pmod{13}$ and we have $\text{ind}_7 2 = 11$ because it’s the only number missing, or alternately because $7^{11} \equiv 2 \pmod{13}$.

(b) Use the table to solve the congruence $3^{x-1} \equiv 5 \pmod{13}$.

**Solution:**
We have:

$$3^{x-1} \equiv 5 \pmod{13}$$
$$\text{ind}_7 3^{x-1} \equiv \text{ind}_7 5 \pmod{12}$$
$$(x - 1)8 \equiv 3 \pmod{12}$$
$$8x - 8 \equiv 3 \pmod{12}$$
$$8x \equiv 11 \pmod{12}$$

which has no solutions because $\gcd(8, 12) = 4 \nmid 11$.

(c) Use the table to solve the congruence $4x^5 \equiv 11 \pmod{13}$.

**Solution:**
We have:

$$4x^5 \equiv 11 \pmod{13}$$
$$\text{ind}_7 (4x^5) \equiv \text{ind}_7 11 \pmod{\phi(13)} = 12$$
$$\text{ind}_7 4 + 5\text{ind}_7 x \equiv \text{ind}_7 11 \pmod{12}$$
$$10 + 5\text{ind}_7 x \equiv 5 \pmod{12}$$
$$5\text{ind}_7 x \equiv 7 \pmod{12}$$
$$\text{ind}_7 x \equiv 11 \pmod{12}$$
$$x \equiv 2 \pmod{13}$$
9. Suppose \( \text{ord}_p a = 3 \), where \( p \) is an odd prime. Show \( \text{ord}_p(a + 1) = 6 \).

**Solution:**
First note that we know \( a^3 \equiv 1 \pmod{p} \) so \( a^3 - 1 \equiv 0 \pmod{p} \). This tells us \( p \mid (a-1)(a^2+a+1) \) so \( p \) divides one of them and since \( a \not\equiv 1 \pmod{p} \) (because \( \text{ord}_p a = 3 \)) we must have \( a^2+a+1 \equiv 0 \pmod{p} \).

With this observe that
\[
(a + 1)^6 \equiv (a^2 + 2a + 1)^3 \equiv (a^2 + a + 1 + a)^3 \equiv (0 + a)^3 \equiv a^3 \equiv 1 \pmod{p}
\]
so that the order divides 6.

- If \( \text{ord}_p(a + 1) = 1 \) then \( a + 1 \equiv 1 \pmod{p} \) so \( a \equiv 0 \pmod{p} \) which is not possible because \( \gcd(a, p) \) must be 1.
- If \( \text{ord}_p(a + 1) = 2 \) then \( (a + 1)^2 \equiv 1 \pmod{p} \) so \( a^2 + 2a + 1 \equiv 1 \pmod{p} \) so \( 0 + a \equiv 1 \pmod{p} \) which is not possible since \( \text{ord}_p a = 3 \).
- If \( \text{ord}_p(a + 1) = 3 \) then \( (a + 1)^3 \equiv 1 \pmod{p} \) so \( a^3 + 3a^2 + 3a + 1 \equiv 1 \pmod{p} \) so \( 1 \equiv a^3 + 3(a^2 + a + 1) - 2 \equiv 1 + 3(0) - 2 \equiv -1 \pmod{p} \) so \( p \mid 2 \) which is not possible since \( p \) is an odd prime.

Thus \( \text{ord}_p(a + 1) = 6 \).

10. Suppose \( r \) is a primitive root modulo \( m \), and \( k \) is a positive integer with \( \gcd(k, \phi(m)) = 1 \). Prove \( r^k \) is also a primitive root.

**Solution:**
Note: The intention is to do this without the theorem from class.

The claim is that \( \text{ord}_m(r^k) = \phi(m) \). Let \( h = \text{ord}_m(r^k) \).

First observe that
\[
(r^k)^{\phi(m)} \equiv (r^{\phi(m)})^k \equiv (1)^k \equiv 1 \pmod{m}
\]
so we know that \( h \mid \phi(m) \).

Second note that \( (r^k)^h \equiv 1 \pmod{m} \) so that \( r^{kh} \equiv 1 \pmod{m} \) so that \( \text{ord}_m r = \phi(m) \) must divide \( kh \). But since \( \gcd(k, \phi(m)) = 1 \) we have \( \phi(m) \mid h \).

Since \( h \mid \phi(m) \) and \( \phi(m) \mid h \) and both are positive we know \( h = \phi(m) \) as desired.