Problem 1. Prove that $\gcd(n, (n-1)!) = 1$ if and only if $n$ is prime.

Solution. \( \implies \) Since $\gcd(n, (n-1)!) = 1$, and $(n-1)! = 1 \cdot 2 \cdot 3 \ldots (n-1)$, $n$ has no common divisor with any number below it which implies that $n$ is prime by the definition of a prime number. Otherwise, $\gcd(n, (n-1)!)>1$ which contradicts the assumption.

\( \impliedby \) Since $n$ is prime, $(n-1)! = 1 \cdot 2 \cdot 3 \ldots (n-1)$ has no factor in common with $n = 1 \cdot n$ (besides 1) and in fact they are all smaller. This means that $n$ and $(n-1)!$ has no common divisors. Thus, $\gcd(n, (n-1)!)=1$. 
**Problem 2.** This question has two sub-problems

(i) Find the additive inverse and multiplicative inverse of 11 in \( \mathbb{Z}_{19} \). Is 11 a perfect square in \( \mathbb{Z}_{19} \) (i.e. is there a value of \( x \in \mathbb{Z}_{19} \) such that \( x^2 \equiv 11 \pmod{19} \))?

**Solution.** Additive inverse = 8. Reason: \( 8 + 11 = 19 \equiv 0 \pmod{19} \).

Multiplicative inverse = 7. Reason: \( 7 \cdot 11 = 77 \equiv 1 \pmod{19} \).

Perfect square = \{7, 12\}. Reason: \( 7^2 = 49 \equiv 11 \pmod{19} \) and \( 12^2 = 144 \equiv 11 \pmod{19} \).

(ii) Show that \( \varphi(12^k) = \varphi(12) \cdot 12^{k-1} \) where \( \varphi \) is the Euler’s totient function.

**Solution.** We have: \( \varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot \varphi(3) = 2^1(2 - 1) \cdot 3^0(3 - 1) = 2 \cdot 2 = 4 \) (by Theorem 2.10 and Theorem 2.11).

By a similar argument, we have: \( \varphi(12^k) = \varphi(2^{2k} \cdot 3^k) = \varphi(2^{2k}) \cdot \varphi(3^k) = 2^{2k-1}(2 - 1) \cdot 3^{k-1}(3 - 1) = 2^{2k} \cdot 3^{k-1} = 4k \cdot 3^{k-1} = 4 \cdot 4^{k-1} \cdot 3^{k-1} = 4 \cdot 12^{k-1} \).

Hence, \( \varphi(12^k) = \varphi(12) \cdot 12^{k-1} \).
Problem 3. Let $a, b, n, n' \in \mathbb{Z}$ with $n > 0$, $n' > 0$, and $\gcd(n, n') = 1$. Show that if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{n'}$, then $a \equiv b \pmod{nn'}$.

Then, use the statement above to show that $(x^{\varphi(y)} + y^{\varphi(x)}) \equiv 1 \pmod{xy}$, where $x, y$ are distinct primes, and $\varphi$ is the Euler’s totient function.

Solution. Let $a \equiv b \pmod{n}$ and $a \equiv b \pmod{n'}$ for some $a, b, nnn' \in \mathbb{Z}$, then $n \mid (a - b)$ and $n' \mid (a - b)$ by the definition of congruence. This implies that $(a - b)$ is a common multiple of $n$ and $n'$ and therefore, $\text{lcm}(nn') \mid (a - b)$ or equivalently, $a \equiv b \pmod{\text{lcm}(nn')}$. Furthermore, we have $nn' = \gcd(nn') \cdot \text{lcm}(nn')$ (proved in Exercise 1.21a, Homework 1), which implies $nn' = 1 \cdot \text{lcm}(nn') = \text{lcm}(nn')$. Hence, $a \equiv b \pmod{nn'}$.

We have $x^{\varphi(y)} \equiv 1 \pmod{y}$ by Euler’s Theorem and $x^{\varphi(y)} \equiv 0 \pmod{x}$. Thus, by Theorem 2.3, we have $(x^{\varphi(y)} + y^{\varphi(x)}) \equiv 1 + 0 = 1 \pmod{y}$. By the same argument, we obtain $(x^{\varphi(y)} + y^{\varphi(x)}) \equiv 1 \pmod{x}$. Previously, we have shown that $a \equiv b \pmod{nn'}$. Thus, letting $a = (x^{\varphi(y)} + y^{\varphi(x)}), b = 1, nn' = xy$, we obtain $(x^{\varphi(y)} + y^{\varphi(x)}) \equiv 1 \pmod{xy}$.
Problem 4. Consider the system of congruences

\[
\begin{align*}
    x &\equiv 6 \pmod{7} \\
    x &\equiv 6 \pmod{11} \\
    x &\equiv 3 \pmod{13}
\end{align*}
\]

Find one solution to the above system. Then, describe all integer solutions to the system.

Solution. Observe that the first two congruences have solution \( x = 6 \) and the Chinese Remainder Theorem (CRT) tells us that this solution is unique modulo \( 7 \cdot 11 = 77 \) because \( \gcd(7, 11) = 1 \). Thus, we can "group" the first two congruences in the system into one, that is, \( x \equiv 6 \pmod{77} \), and we obtain the new system:

\[
\begin{align*}
    x &\equiv 6 \pmod{77} \\
    x &\equiv 3 \pmod{13}
\end{align*}
\]

By the definition of congruence and for some integers \( a \) and \( b \), we rewrite the system as follow:

\[
\begin{align*}
    x &= 6 + 77a \\
    x &= 3 + 13b
\end{align*}
\]

In other words, \( 6 + 77a = 3 + 13b \) \( \iff \) \( 77a - 13b = -3 \). Clearly, this equation has a solution because \( \gcd(77, 13) = 1 \) (by Theorem 2.5) and now, we want to find integers \( a \) and \( b \) that satisfy this linear combination.

To this end, we will first find integers \( a' \) and \( b' \) that satisfy \( 77a' + 13b' = 1 \), and clearly this equation has a solution because of the same reason above. We can then obtain \( a = (-3)a' \) and \( b = 3b' \) by multiplying both sides of the previous equation by \(-3\), namely, \( 77(-3a') - 13(3b') = -3 \).

We run Extended Euclidean Algorithm (EEA) on input \( (77, 13) \) and obtain \( a' = -1 \) and \( b' = 6 \). Sanity check: \( 77 \cdot (-1) + 13 \cdot 6 = -77 + 78 = 1 \). (I did not include my calculation here for simplicity but you have to show the steps of EEA in your paper). Therefore, we obtain \( a = (-3)a' = 3 \) and \( b = 3b' = 18 \) which satisfy \( 77a - 13b = 77 \cdot 3 - 13 \cdot 18 = 231 - 234 = -3 \).

Substitute \( a = 3 \) to \( x = 6 + 77a \) we obtain \( x = 237 \) which is one solution to the given system. Since 7, 11, and 13 are pairwise relatively prime, the solution of the given system is unique modulo \( 7 \cdot 11 \cdot 13 = 1001 \) by CRT. We have shown that \( x = 237 \) is one solution, and therefore; we can describe all solutions as \( x \equiv 237 \pmod{1001} \).