1. Find all solutions to the following system of linear congruences using the technique in the proof of Theorem 5.26 in Apostol

\[
\begin{align*}
    x &\equiv 1 \pmod{4} \\
    x &\equiv 0 \pmod{3} \\
    x &\equiv 5 \pmod{7}
\end{align*}
\]

2. Cowardly Pirates: A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. There was a fierce discussion where the pirates debated who should get the extra coins and one pirate got scared and ran away. The coins were redistributed amongst the remaining pirates but there were 10 coins left. Again another argument developed and yet another cowardly pirate ran away. The total set of coins could then be evenly divided amongst the pirates who were brave enough to have stayed. What is the minimum number of coins that could have been stolen?

3. For the following system of congruences, simplify them so that the Chinese Remainder Theorem applies and then find all solutions

\[
\begin{align*}
    5x &\equiv 1 \pmod{7} \\
    3x &\equiv 2 \pmod{5} \\
    7x &\equiv 1 \pmod{3}
\end{align*}
\]

4. Let \( m_1 \) and \( m_2 \) be integers greater than 1 and consider the system of congruences

\[
\begin{align*}
    x &\equiv b_1 \pmod{m_1} \\
    x &\equiv b_2 \pmod{m_2}
\end{align*}
\]

(a) Show that this system of congruences has a solution if and only if \( b_1 \equiv b_2 \pmod{g} \) where \( g = \text{lcm}(m_1, m_2) \).

(b) Show that if the system of congruences has a solution then it is unique module \( \text{lcm}(m_1, m_2) \).

(Recall from exam 1 that \( \text{lcm}(m_1, m_2) = m_1 m_2 / \gcd(m_1, m_2) \) is the least common multiple of \( m_1, m_2 \) and use the result from exam 1 that if \( m_1 | y \) and \( m_2 | y \) then \( \text{lcm}(m_1, m_2) | y \).)

5. If \( f \) is a polynomial and the congruence

\[
f(x) \equiv 0 \pmod{m}
\]

has \( m \) solutions then prove that any integer whatsoever is a solution.

6. Suppose that \( f \) is a polynomial and that the congruence

\[
f(x) \equiv k \pmod{m}
\]

has exactly \( \nu(k) \) solutions modulo \( m \). Prove that \( \sum_{k=1}^{m} \nu(k) = m \).

(continued on next page)
7. Finding a factor of a composite integer using the Pollard \( p - 1 \) method. Suppose that we seek a non-trivial factor (a factor other than \( \pm 1 \) or \( \pm m \)) of the composite odd integer \( m \). Let \( d_n = (2^n - 1, m) \). A calculator or computer will be needed for part c below. But note that computing \( d_n \) is relatively fast because it is fast to find greatest common divisors and because once \( 2^{(n-1)!} \) is found we can replace it by its least absolute residue modulo \( m \) (find \( Y \) so \( 2^{(n-1)!} \equiv Y \pmod{m} \) and \( -m/2 < Y < m/2 \)) and then \( 2^n! \) can be found modulo \( m \) using \( 2^n! = (2^{(n-1)!})^n \equiv Y^n \pmod{m} \).

(a) Show that if \( 1 < d_n < m \) then we have found a non-trivial factor of \( m \).

(b) Show that if \( p \) is a prime factor of \( m \) and \( (p-1) \mid n! \) then \( p \mid d_n \).
   (So we can find a non-trivial factor of \( m \) using \( d_n \) unless \( d_n = m \).)

(c) Based on part b, this technique is particularly fast for composite numbers \( m \) which have a prime factor \( p \) for which \( p - 1 \) may be factored into a product of small primes. To see an example of this, apply the technique to \( m = 2867 \) by calculating \( d_1, d_2, \ldots \) consecutively until a non-trivial factor is found. State the first factor found and the \( n \) for which it is found and show that these satisfy the condition in part b that \( p - 1 \mid n! \).