1. Solve the congruence \(13x \equiv 210 \pmod{240}\) in two different ways.

   (a) Method 1: Use the Euclidean algorithm (or Euler’s method) to solve the associated first order linear equation.

   **Solution:** We solve \(13x = 210 + 240y\) for \(x\) (and \(y\)). Using Euler’s method, \(x = \frac{210 + 240y}{13} = 16 + 18y + \frac{2 + 6y}{13}\). Let \(z = \frac{13z - 2}{6}\). Then \(z = 2\), giving \(y = 4\), \(x = 16 + 72 + 2 = 90\). Since 13 is prime to 240, the answer is \(x \equiv 90 \pmod{240}\).

   (b) Method 2: Break the congruence into congruences \((\pmod{15})\) and \((\pmod{16})\), solve each of these, and put the solutions together via the Chinese Remainder Theorem.

   **Solution:** We use 240 = \(15 \times 16\). The original congruence is equivalent to the system \(13x \equiv 210 \pmod{15}\), \(13x \equiv 210 \pmod{16}\). These simplify to \(13x \equiv 0 \pmod{15}\), \(13x \equiv 2 \pmod{16}\). The first congruence has solution \(x \equiv 0 \pmod{15}\). For the second, the easiest approach is to note that \(5 \times 13 = 65 \equiv 1 \pmod{16}\), and multiply both sides of the original congruence by 5. This gives \(x \equiv 10 \pmod{16}\). Alternatively, convert to a linear Diophantine equation, say \(13x + 16y = 2\). If we use the Euclidean algorithm, \(16 = 13 \times 1 + 3\), \(13 = 3 \times 4 + 1\) so \(1 = 13 - 3 \times 4 = 13 - 4(16 - 13) = 5 \times 13 - 4 \times 16\). Doubling, \(2 = 10 \times 13 - 40 \times 16\), and again \(x = 10 \pmod{16}\). Finally, we put \(x \equiv 0 \pmod{15}\), \(x \equiv 10 \pmod{16}\) together: From the first, write \(x = 15y\). Putting this into the second, \(15y \equiv 10 \pmod{16} \rightarrow -y \equiv 10 \pmod{16} \rightarrow y \equiv -1 \equiv 6 \pmod{16}\), or \(y = 6 + 16z\). Thus, \(x = 15y = 90 + 240z\), or \(x \equiv 90 \pmod{240}\).

2. Find (with proof) all positive integers \(n\) with \(\phi(n) = 20\).

   **Solution:** If \(n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\), then \(\phi(n) = p_1^{a_1 - 1}(p_1 - 1) \cdots p_k^{a_k - 1}(p_k - 1)\). In particular, if \(p \mid n\) then \(p - 1 \mid \phi(n)\). Moreover, if \(p^2 \mid n\) then \(p \mid \phi(n)\). Since the divisors of 20 are 1, 2, 4, 5, 10, 20, the only possible prime divisors of \(n\) are 2, 3, 5, 11. Since 3 \(\nmid 20\) and 11 \(\nmid 20\) we know 3 \(\nmid n\) and 11 \(\nmid n\). One way to solve this problem would be to let \(n = 2^a 3^b 5^c 11^d\). We know \(b \leq 1\) and \(d \leq 1\). Also, \(c \leq 2\) and \(a \leq 3\) (because \(\phi(5^3)\) and \(\phi(2^4)\) are not divisors of 20). This leads to 24 possible cases. One can check all 24 cases to see which ones work.
Alternatively, we do a little more thinking. One more thing we know: If \( q \) is a prime and \( q \mid \phi(n) \), then from the formula for \( \phi(n) \), we know that either \( q \mid n \) or \( q \mid p - 1 \) for some prime divisor \( p \) of \( n \). Since \( 5 \mid 20 \), either \( 5 \mid n \) or \( 5 \mid p - 1 \) for some divisor \( p \) of \( n \). If \( 5 \mid n \), we can’t have \( n = 5^m \) with \( m \) prime to 5 because in this case, \( 20 = \phi(5m) = 4\phi(m) \rightarrow \phi(m) = 5 \), and as we showed in the last homework, if \( \phi(m) \neq 1 \) then \( \phi(m) \) is even. This means we need \( 5^2 \) to divide \( n \) so \( n = 5^2m \) with \( m \) prime to 5. Here, \( \phi(n) = \phi(25)\phi(m) = 20\phi(m) \rightarrow \phi(m) = 1 \), and \( m = 1 \) or 2, giving solutions \( n = 25, 50 \).

If \( 5 \not\mid n \) then \( 11 \mid n \) because 11 is the only prime in our list for which \( 5 \mid p - 1 \). We must have \( n = 11m \), where \( m \) is prime to 11 since \( 11^2 \not\mid n \), so \( 20 = \phi(11m) = 10\phi(m) \). Thus, \( \phi(m) = 2 \), which only happens if \( m = 3, 4, \) or 6. This is because 2 and 3 are the only primes with \( p - 1 \mid 2 \), and as \( 3 \not\mid 2 \), the only cases are \( m = 2^k \) or \( m = 3 \times 2^k \), and we can quickly check to get the three values listed above. So if \( 11 \mid n \) then \( n = 33, 44, \) or 66.

To sum up, the list of possible \( n \) values is 25, 50, 33, 44, 66.

3. Solve each of the following systems of congruences.

(a)\[
\begin{align*}
x & \equiv 1 \pmod{3} \\
x & \equiv 3 \pmod{5} \\
x & \equiv 5 \pmod{7}.
\end{align*}
\]

**Solution:** This problem has a quick tricky solution: we can rewrite things as \( x \equiv -2 \pmod{3}, \ x \equiv -2 \pmod{5}, \ x \equiv -2 \pmod{7} \), so the solution must be \( x \equiv -2 \pmod{105} \) or \( x \equiv 103 \pmod{105} \).

Alternatively, using the iterative approach I mentioned in class, \( x = 1 + 3k \equiv 3 \pmod{5} \rightarrow 3k \equiv 2 \pmod{5} \rightarrow k \equiv 4 \pmod{5} \). This means \( x = 1 + 3(4 + 5j) = 13 + 15j \). Using the last equivalence, \( 13 + 15j \equiv 5 \pmod{7} \rightarrow -1 + j \equiv 5 \pmod{7} \rightarrow j \equiv 6 \pmod{7} \). If we write \( j = 6 + 7m \), then \( x = 13 + 15(6 + 7m) = 103 + 105m \), so \( x \equiv 103 \pmod{105} \).
(b) 
\[ \begin{align*} 
& x \equiv 1 \pmod{2} \\
& x \equiv 2 \pmod{3} \\
& x \equiv 3 \pmod{5} \\
& x \equiv 4 \pmod{7}. 
\end{align*} \]

**Solution:** As above, \( x = 1 + 2r \equiv 2 \pmod{3} \rightarrow 2r \equiv 1 \pmod{3} \rightarrow r \equiv 2 \pmod{3} \). So \( x = 1 + 2(2 + 3k) = 5 + 6k \equiv 3 \pmod{5} \rightarrow k \equiv 3 \pmod{5} \rightarrow x = 5 + 6(3 + 5j) = 23 + 30j \). Next, \( 23 + 30j \equiv 4 \pmod{7} \rightarrow 2 + 2j \equiv 4 \pmod{7} \rightarrow 2j \equiv 2 \pmod{7} \rightarrow j \equiv 1 \pmod{7} \). Thus, \( x = 23 + 30(1 + 7m) = 53 + 210m \), or \( x \equiv 53 \pmod{210} \).

(c) 
\[ \begin{align*} 
& x \equiv 1 \pmod{12} \\
& x \equiv 4 \pmod{21} \\
& x \equiv 18 \pmod{35}. 
\end{align*} \]

**Solution:** Consistency/nonconsistency should fall out of the math. \( x = 1 + 12k \equiv 4 \pmod{21} \rightarrow 12k \equiv 3 \pmod{21} \). Since 3 divides each of the terms, \( 4k \equiv 1 \pmod{7} \) or \( k \equiv 2 \pmod{7} \) giving \( x = 1 + 12(2 + 7j) = 25 + 84j \). Moving to the last congruence, \( 25 + 84j \equiv 18 \pmod{35} \rightarrow 14j \equiv 28 \pmod{35} \rightarrow j \equiv 2 \pmod{5} \). I am using here, the rule that if \( d = \gcd(c, m) \), then \( ac \equiv bc \pmod{m} \rightarrow a \equiv b \pmod{m/d} \). We have \( x = 25 + 84(2 + 5m) = 193 + 420m \), or \( x \equiv 193 \pmod{420} \). Note here, that the final congruence is modulo \( \text{lcm}(12, 21, 35) = 420 \) not 12 \( \times \) 21 \( \times \) 35 = 8820.

(d) 
\[ \begin{align*} 
& x \equiv 2 \pmod{9} \\
& x \equiv 8 \pmod{15} \\
& x \equiv 10 \pmod{25}. 
\end{align*} \]

**Solution:** Simplest is to note that \( x \equiv 8 \pmod{15} \) and \( x \equiv 10 \pmod{25} \) are inconsistent (but the first two congruences ARE consistent with each other). To see this, \( x \equiv 8 \pmod{15} \rightarrow x = 8 + 15k \), and plugging this into the third congruence, \( 8 + 15k \equiv 10 \pmod{25} \rightarrow 15k \equiv 2 \pmod{25} \). Here, \( \gcd(15, 25) = 5 \), but 5 \( \nmid \) 2. Thus, there are no solutions to this congruence.
4. Find a number \( n \) such that \( 3^2 \mid n \), \( 4^2 \mid n + 1 \), \( 5^2 \mid n + 2 \).

**Solution:** In terms of congruences, \( n \equiv 0 \pmod{9} \), \( n \equiv 15 \pmod{16} \), \( n \equiv 23 \pmod{25} \). As a change, let’s go from largest modulus to smallest. We have \( n = 23 + 25k = 15 \pmod{16} \) \( \rightarrow 9k = 8 \pmod{16} \). We might notice that \( 81 \equiv 1 \pmod{16} \), which would tell us to multiply this congruence by 9, to get \( k \equiv 8 \pmod{16} \). Suppose we did not notice this. Instead, we could convert to a Diophantine problem: \( 9k \equiv 8 \pmod{16} \) is equivalent to \( 9k + 16x = 8 \). Applying Euler’s method, \( k = \frac{8 - 16x}{9} = -x + \frac{8 - 7x}{9} \rightarrow 9y + 7x = 8 \rightarrow x = \frac{8 - 9y}{7} = 1 - y + \frac{1 - 2y}{7} \). Rather than continuing, I will note that \( y = -3 \) makes \( \frac{1 - 2y}{7} \) an integer, so we could let \( y = -3 \rightarrow x = 5 \rightarrow k = -8 \). Since \( -8 \equiv 8 \pmod{16} \), we again get \( k \equiv 8 \pmod{16} \).

Continuing, \( n = 23 + 25k = 23 + 25(8 + 16j) = 223 + 400j \equiv 0 \pmod{9} \), or \( 7 + 4j \equiv 0 \pmod{9} \) \( \rightarrow 4j \equiv 2 \pmod{9} \) \( \rightarrow j \equiv 5 \pmod{9} \). One could get this by trial-and-error, or by multiplying by 7 \((4 \times 7 \equiv 1 \pmod{9})\) Thus, \( n = 223 + 400(5 + 9m) = 2223 + 3600m \). So \( n = 2223 \) works, as does any multiple of 3600 added to 2223.

Extra credit:

5. Show that for each prime \( p \geq 5 \), if we let \( n_p = \frac{4^p - 1}{3} \), then \( n_p \) is a base 2 pseudoprime.

**Solution:** First, note that \( n_p \) actually is an integer: \( 4^p - 1 \equiv 1 - 1 = 0 \pmod{3} \), so the numerator is divisible by 3. Next, we need \( n_p \) to be composite. Since \( 4^p - 1 = (2^p - 1)(2^p + 1) \), and 3 divides this number, one of the two terms in the product is divisible by 3. Since \( p \geq 5 \), even when divided by 3, the resulting thing will be larger than 1. Thus, \( n_p \) will be a product of integers larger than 1. Finally, we need \( 2^{n_p - 1} \equiv 1 \pmod{n_p} \). To establish the congruence, note that \( 2^{n_p - 1} = 2^{(4^p - 4)/3} \). Since \( p \) is prime, by Fermat’s Little Theorem, \( 4^p - 4 \) is divisible by \( p \). It is also divisible by 3 (for the same reason the numerator of \( n_p \) is divisible by 3) and it is even, so \( \frac{4^p - 4}{3} = 2kp \) for some integer \( k \). Thus, \( 2^{n_p - 1} = 2^{2kp} = (4^p)^k = (3n_p + 1)^k \equiv (0 + 1)^k \pmod{n_p} \equiv 1 \pmod{n_p} \), as desired.

6. Generalize the previous problem: Prove that for every integer \( b \geq 2 \), there are infinitely many pseudoprimes base \( b \).

**Solution:** The trick is to see what replaces \( n_p = \frac{4^p - 1}{3} \), the case for 2. In fact, \( n_p = \frac{b^{2p} - 1}{b^2 - 1} \), works for \( b \), by a very similar proof.