1. Use the CRT to find the second smallest positive integer solution to the following system:

$$\begin{aligned} 3x &\equiv 6 \bmod 15 \\ 5x &\equiv 4 \bmod 6 \\ x+1 &\equiv 2 \bmod 7 \end{aligned}$$

Solution: We rewrite and solve these individually as:

$$\begin{aligned} x &\equiv 2 \bmod 5 \\ x &\equiv 2 \bmod 6 \\ x &\equiv 1 \bmod 7 \end{aligned}$$

Then $M = (5)(6)(7) = 210$, $M_1 = 42$, $M_2 = 35$ and $M_3 = 30$. We then solve:

$$\begin{aligned} 42y_1 &\equiv 1 \bmod 5 \text{ which is } 2y_1 \equiv 1 \bmod 5 \text{ so } y_1 = 3. \\ 35y_2 &\equiv 1 \bmod 6 \text{ which is } 5y_2 \equiv 1 \bmod 6 \text{ so } y_2 = 5. \\ 30y_3 &\equiv 1 \bmod 7 \text{ which is } 2y_3 \equiv 1 \bmod 7 \text{ so } y_3 = 4. \end{aligned}$$

So all solutions are given by

$$x \equiv (42)(3)(2) + (35)(5)(2) + (30)(4)(1) \equiv 722 \equiv 92 \bmod 210$$

So that the second smallest solution is $x = 92 + 210 = 302$.

2. Find each of the following.

   (a) The least nonnegative residue of $(14!)4^{371}$ modulo 17.
   Solution: By Wilson's Theorem:

$$\begin{aligned} 16! &\equiv -1 \bmod 17 \\ (16)(15)14! &\equiv -1 \bmod 17 \\ (-1)(-2)14! &\equiv -1 \bmod 17 \\ (-2)14! &\equiv 1 \bmod 17 \\ (-9)(-2)14! &\equiv -9 \bmod 17 \\ 14! &\equiv 8 \bmod 17 \end{aligned}$$

   By Fermat's Little Theorem $4^{16} \equiv 1 \bmod 17$ so then:

$$4^{371} \equiv (4^{16})^{23}4^3 \equiv 4^3 \equiv 64 \equiv 13 \bmod 17$$

   Thus

$$(14!)4^{371} \equiv (8)(13) \equiv 2 \bmod 17$$

   (b) The least nonnegative residue of 1234^5 modulo 1236.
   Solution: We have:

$$1234^5 \equiv (-2)^5 \equiv -32 \equiv 1204 \bmod 1236$$

3. Find all incongruent solutions, if any, modulo the original modulus, to the following:

   (a) $5x \equiv 6 \bmod 16$
   Solution: Since $\gcd(5,16) = 1 \mid 6$ there is one solution. By testing we find it is $x = 14$.

   (b) $2x \equiv 18 \bmod 46$
   Solution: Since $\gcd(2,46) = 2 \mid 18$ there are two solutions. By testing one is $x = 9$ so all are $x = 9 + \frac{46}{2}k$ for $k = 0, 1$, or specifically $x = 9$ and $x = 32$.

   (c) $13^{162}x \equiv 2 \bmod 13^{163}$
   Solution: Since $\gcd(13^{162}, 13^{163}) \nmid 2$ there are no solutions.

4. Calculate the following. Answers do not need to be simplified!

   (a) $\phi(6!7!)$
   Solution: The prime factors involved in 6! and 7! are only 2,3,5,7 and so

$$\phi(6!7!) = 6!7!\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

   (b) $\sigma(10^{10})$
   Solution: Since $10^{10} = 2^{10}5^{10}$ we have

$$\sigma(10^{10}) = \sigma(2^{10})\sigma(5^{10}) = \frac{2^{11}-1}{2-1}\frac{5^{11}-1}{5-1}$$

   (c) $\tau(10!)$
   Solution: Since $10! = (10)(9)(8)(7)(6)(5)(4)(3)(2)(1) = 2^8 3^4 5^2 7^1$ we have

$$\tau(10!) = (8+1)(4+1)(2+1)(1+1)$$

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

   Solution: Since $\gcd(3,91) = 1$, Euler's Theorem tells us that $3^{\phi(91)} \equiv 1 \bmod 91$. We find $\phi(91) = \phi(7 \cdot 13) = (6)(12) = 72$ so then to check it's a Pseudoprime:

$$3^{91-1} \equiv 3^{90} \equiv 3^{72}3^{18} \equiv 3^{18} \bmod 91$$

   A bit more work to do. Note:

$$\begin{aligned} 3^1 &\equiv 3 \bmod 91 \\ 3^2 &\equiv 9 \bmod 91 \\ 3^4 &\equiv 81 \bmod 91 \\ 3^8 &\equiv 81^2 \equiv (-10^2) \equiv 100 \equiv 9 \bmod 91 \\ 3^{16} &\equiv 81 \bmod 91 \end{aligned}$$

   and so finally

$$3^{91-1} \equiv 3^{18} \equiv 3^{16}3^2 \equiv (81)(9) \equiv (-10)(9) \equiv -90 \equiv 1 \bmod 91$$

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

   Solution: If $\gcd(6,n) = 1$ then $\gcd(2,n) = 1$ and $\gcd(3,n) = 1$ and so then

$$\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$$

   and

$$2\phi(2n) = 2\phi(2)\phi(n) = 2\phi(n)$$

   So they're equal.

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

   Solution: If $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ then $\tau(n) = (\alpha_1 + 1)...(\alpha_k + 1)$. For this to equal 12 it must be a factorization of 12 and thus could only be (12) or (2)(6) or (3)(4) or (2)(2)(3).

   If it's (12) then $n = p_1^{11}$.

   If it's (2)(6) then $n = p_1 p_2^5$.

   If it's (3)(4) then $n = p_1^2 p_2^3$.

   If it's (2)(2)(3) then $n = p_1 p_2 p_3^2$.

8. Prove (using the definition of congruence) or disprove (by counterexample) each of the following. Hint: One is true, two are false.

   (a) If $ac \equiv bc \bmod m$ with $c \not\equiv 0 \bmod m$ then $a \equiv b \bmod m$.
   Solution: False, for example $(2)(2) \equiv (5)(2) \bmod 6$ but $2 \not\equiv 5 \bmod 6$.

   (b) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.
   Solution: True. If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $m \mid (a - b)$ and $m \mid (b - c)$ and so $m \mid (a - b) + (b - c)$ so $m \mid (a - c)$ yielding $a \equiv c \bmod m$.

   (c) If $a \equiv b \bmod m$ then $m \mid (a + b)$.
   Solution: False. For example $1 \equiv 1 \bmod 7$ but $7 \nmid (1 + 1)$.

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

   Solution: Since n and pn are perfect, $\sigma(n) = 2n$ and $\sigma(pn) = 2pn$.

   We proceed by contradition: If $\gcd(p, n) = 1$ then

   $$\sigma(pn) = \sigma(p)\sigma(n) = (p + 1)2n = 2pn + 2n \neq \sigma(pn)$$

   a contradiction.

10. Prove that for a fixed k that $\phi(n) = k$ can have at most a finite number of solutions.

    Solution: Since it's easier we'll show that $\phi(n) \leq k$ can have at most a finite number of solutions, since clearly if $\phi(n) = k$ then $\phi(n) \leq k$.

    Suppose p^α appears in the prime factorization of n, so then $n = p^\alpha N$ where N is the rest. Then:

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

    First note that this is greater than or equal to $p - 1$, so in order to guarantee that $\phi(n) \leq k$ we must have $p - 1 \leq k$ or $p \leq k + 1$ which means there are only a finite number of different primes which can appear in the prime factorization of n.

    Second observe that this is greater than or equal to $p^{\alpha-1}$, so in order to guarantee that $\phi(n) \leq k$ we must have $p^{\alpha-1} \leq k$ or $\alpha - 1 \leq \log_p k$ or $\alpha \leq 1 + \log_p k$.

    Therefore there are only a finite number of primes available and each can be only to a finite number of powers, yielding only a finite number of possible n.

    Explanatory Note: If you're interested in how this works by example, consider $\phi(n) \leq 10$. The first part states that the primes in the prime factorization of n must be less than or equal to 11, meaning we can only use 2,3,5,7,11. The second part states that the exponent of 2 must be less than $1+\log_2(10) \approx 4.32$ (so either $1, 2, 3, 4$), the exponent of 3 must be less than $1+\log_3(10) \approx 3.10$ (so either $1, 2, 3$), the exponent of 5 must be less than $1 + \log_5(10) \approx 2.43$ (so $1, 2$), the exponent of 7 must be less than $1 + \log_7(10) \approx 2.18$ (so $1, 2$), the exponent of 11 must be less than $1 + \log_{11}(10) \approx 1.96$ (so 1).