**Problem 1.** 1. We see that

\[ 5^2 = 25 \equiv 1 \pmod{8} \]

Thus by exponentiating the above congruence we get

\[ (5^2)^{10} \equiv 1 \pmod{8} \]

Therefore

\[ 5^{21} = 5 \times 5^{20} \equiv 5 \times 1 \equiv 5 \pmod{8}. \]

2. We have that \( 201 = 5 \times 40 + 1 \). First notice that

\[ 31 \equiv -2 \pmod{33} \]

Thus

\[ (31)^5 \equiv (-2)^5 \equiv -32 \equiv 1 \pmod{33} \]

Now raising both sides to the 40-th power we get

\[ ((31)^5)^{40} \equiv (1)^{40} \equiv 1 \pmod{33} \]

3. The last two digits of any number belongs to the set \{00, 01, 02, 03, 04, \ldots, 97, 98, 99\}. This set can be easily identified as the set of numbers modulo 100. Thus to find the last two digits of \( 9^{30} \) we must find its modulo w.r.t 100. We have

\[ 9^5 = 59049 \equiv 49 \pmod{100} \]

Therefore

\[ 9^{10} = (9^5)^2 \equiv 49^2 = 2401 \equiv 1 \pmod{100} \]

Thus

\[ 9^{30} = (9^{10})^3 \equiv 1^3 \equiv 1 \pmod{100} \]

So the last two digits of \( 9^{30} \) are 0, 1.

**Problem 2.** We know from the Bezout’s theorem that for any integers \( a, b \)

\[ \gcd(a, b) = \alpha a + \beta b \]

for some integers \( \alpha, \beta \). Note that if the \( \gcd(a, b) = 1 \), then we have that

\[ \alpha a = -\beta b + 1 \]

Thus

\[ \alpha a \equiv 1 \pmod{b} \]

As a result we have that \( \alpha = (a)^{-1} \pmod{b} \).
1. Using the extended Euclid’s algorithm we have
\[
gcd(5, 26) = 1 = (-5)5 + (1)26
\]
Thus \(-5 \equiv 21 \equiv (5)^{-1} \pmod{26}\).

2. Using the extended Euclid’s algorithm we have
\[
gcd(11, 36) = 1 = (-13)11 + (4)36
\]
Thus \(-13 \equiv 23 \equiv (11)^{-1} \pmod{36}\).

3. Using Euclid’s algorithm we have
\[
gcd(14, 35) = 7 \neq 1
\]
So, \(14^{-1} \pmod{35}\) does not exist.

**Problem 3.** 1. Since \(m\) is a prime number the only integers among \(1, 2, \ldots, m^4\) which have a factor common with \(m\) are the multiples of \(m\). The multiples of \(m\) less than \(m^4\) are \(\{1 \cdot m, 2 \cdot m, 3 \cdot m, \ldots, m^3 \cdot m\}\). Thus there are \(m^3\) multiples of \(m\). As a result
\[
\phi(m^4) = m^4 - m^3 = m^3(m - 1).
\]

2. Since \(p\) and \(q\) are prime numbers, the only positive integer factors of \(pq\) are \(1, p, q\) and \(pq\). So to find \(\phi(pq)\) we must count the multiples of \(p, q, p.q\) and subtract it from \(pq\). Among the numbers \(1, 2, \ldots, pq\) there are \(\frac{pq}{p} = q\) multiples of \(p\) and there are \(\frac{pq}{q} = p\) multiples of \(q\). Since \(p\) and \(q\) are distinct prime numbers, if for an integer number \(n\), both \(p\) and \(q\) are factors of \(n\) then \(n\) is divisible by product of them (i.e \(n\) is divisible by \(pq\)). This means that the only number among \(1, 2, 3, \ldots pq\) which is divisible by both numbers \(p\) and \(q\) is \(pq\). Therefore,
\[
\phi(pq) = pq - p - q + 1 = (p - 1)(q - 1)
\]

**Problem 4.** 1. \(42 = 3 \times 3 \times 7\). We know that if \(m, n\) are relatively prime then \(\phi(mn) = \phi(m)\phi(n)\). Thus \(\phi(42) = \phi(2)\phi(3)\phi(7)\). And for any prime number \(m\), \(\phi(m) = m - 1\). Thus \(\phi(42) = (2 - 1)(3 - 1)(7 - 1) = 12\).

2. We know from the Euler’s theorem that if \(a, m\) are relatively prime then
\[
a^{\phi(m)} \equiv 1 \pmod{m}.
\]
This implies that
\[
a^{\phi(m)-1}a \equiv 1 \pmod{m}.
\]
Thus \(a^{\phi(m)-1} \equiv a^{-1} \pmod{m}\). In this problem since \(11, 42\) are relatively prime, we have
\[
11^{\phi(42)-1} = 11^{11} \equiv 11^{-1} \pmod{42}
\]
using the fact that \(\phi(42) = 12\). But
\[
11^2 = 121 \equiv -5 \pmod{42}
\]
\[
11^4 \equiv (-5)^2 \equiv 25 \pmod{42}
\]
\[
11^6 = (11^4) \times (11^2) \equiv 25 \times (-5) \equiv -125 \equiv 1 \pmod{42}
\]
\[
11^{11} = (11^6) \times (11^4) \times 11 \equiv (1)(25)(11) \equiv 275 \equiv 23 \pmod{42}
\]
Thus \(23 \equiv 11^{-1} \pmod{42}\).
Problem 5. 1. We enumerate $x$ starting from 0 to see that $x = 5$ satisfies the congruence equation.

2. By Euler’s theorem we know that $3^{\phi(17)} \equiv 1 \pmod{17}$ since $\gcd(3, 17) = 1$. Therefore $3^{16} \equiv 1 \pmod{17}$ Thus

$$3^{5+16} = 3^5 \times 3^{16} \equiv 5 \times 1 \equiv 5 \pmod{17}.$$

This means $x = 5 + 16 = 21$ is another solution. In fact, the same method gives us infinitely many solutions for this congruence equation.

3. This congruence equation does not have a solution for $x$. To prove this let us assume that there exists a number $x \geq 0$ such that $3^x \equiv 5 \pmod{15}$. This implies that 15 divides $3^x - 5$. Therefore 3 also divides $3^x - 5$ but this is not possible since $3^x$ is divisible by 3 but 5 is not.