Esercizio 1. Find the multiplicative inverse of 22 modulo 135.

Solution
We perform the Euclidean algorithm for the GCD:

\[ 135 = 22 \cdot 6 + 3 \]
\[ 22 = 3 \cdot 7 + 1 \]

and going backwards, we get

\[ 1 = 22 - 3 \cdot 7 = 22 - (135 - 22 \cdot 6) \cdot 7 = 22 \cdot (1 + 6) - 135 \cdot 7 = 22 \cdot 43 - 135 \cdot 7 \]

Therefore, \( 22 \cdot 43 \equiv 1 \mod (135) \), namely \( [22]^{-1}_{135} = 43 \).

Esercizio 2. Compute the remainder of \( 3^{64} \) in the division by 67.

Solution
We have \( 64 = 2^6 \). Hence

\[ 3^2 = 9 \]
\[ 3^4 = 9^2 = 81 \equiv 14 \mod (67) \]
\[ 3^8 = 14^2 = 196 \equiv 62 \equiv -5 \mod (67) \]
\[ 3^{16} = (-5)^2 = 25 \mod (67) \]
\[ 3^{32} = 25^2 = 625 \equiv 22 \mod (67) \]
\[ 3^{64} = 22^2 = 484 \equiv 15 \mod (67) \]

Esercizio 3. Solve the following system of congruence equations:

\[ \begin{cases} 
    x \equiv 1 \mod (3) \\
    x \equiv 2 \mod (5) \\
    x \equiv 3 \mod (7) 
\end{cases} \]

Solution
The numbers 3, 5 and 7 are pairwise coprime. Hence, by the Chinese Remainder Theorem there exists a unique solution modulo \( 3 \cdot 5 \cdot 7 = 105 \), and it is

\[ x = 105 \cdot \left( \frac{105}{3} \right)^{-1} \cdot 1 + 105 \cdot \left( \frac{105}{5} \right)^{-1} \cdot 2 + 105 \cdot \left( \frac{105}{7} \right)^{-1} \cdot 3 \]
\[ = 35 \cdot 2 \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 3 = 70 + 42 + 45 = 157 \equiv 52 \mod 105 \]

Esercizio 4. Prove that the following identity holds for every \( n \in \mathbb{N} \):

\[ \sum_{i=0}^{n} i \binom{n}{i} = n \cdot 2^{n-1} \]

Solution
By the Binomial Theorem we have

\[ (1 + x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \]
Taking the derivative of both sides we get
\[ n(1 + x)^{n-1} = \sum_{i=0}^{n} \binom{n}{i} i x^{i-1} \]

Letting \( x = 1 \) we get
\[ n^{2n-1} = \sum_{i=0}^{n} \binom{n}{i} \]

**Esercizio 5.** For every \( k \geq 1 \) and every odd prime \( p \), find the number of solutions of the following congruence equation
\[ x^3 - x^2 + x - 1 \equiv 0 \pmod{p^k}. \]

**Solution**
We start by solving the equation modulo \( p \), which is, after factoring \( x - 1 \),
\[ (x - 1)(x^2 + 1) \equiv 0 \pmod{p} \]

This equation has one solution \( x = 1 \) for every prime \( p \), and the solutions of the equation
\[ x^2 \equiv -1 \pmod{p} \]

We know that this equation has (two) solutions if and only if \( p \equiv 1 \pmod{4} \) (and they are \( x = \pm \alpha \), where \( \alpha \equiv \frac{p-1}{2} \pmod{p} \)). Hence, the congruence equation mod \( p \) has:
(i) for \( p \equiv 1 \pmod{4} \), three solutions modulo \( p \), namely \( x = 1, \pm \alpha \),
(ii) for \( p \equiv 3 \pmod{4} \), one solution modulo \( p \), namely \( x = 1 \).

Next, let us see whether these solutions are singular or not. We have
\[ f'(x) = 3x^2 - 2x + 1 \]

Hence,
\[ f'(1) = 3 \cdot 1^2 - 2 \cdot 1 + 1 = 2 \not\equiv 0 \pmod{p} \]

so 1 is a non-singular solution. Furthermore,
\[ f'(\pm \alpha) = 3 \cdot \alpha^2 \pm 2 \cdot \alpha + 1 \equiv -3 \mp 2\alpha + 1 = -2 \mp 2\alpha = -2(\pm \alpha + 1) \not\equiv 0 \pmod{p} \]

since \(-2 \not\equiv 0 \pmod{p}\) and \( \alpha \not\equiv \pm 1 \pmod{p} \) (because \((\pm 1)^2 = 1 \neq -1 \)). Hence, also \( \pm \alpha \) are a non-singular solutions. Therefore, each of these non-singular solution lifts to a unique solution modulo \( p^k \), for every \( k \geq 1 \). In conclusion, for every \( k \geq 1 \),
(i) for \( p \equiv 1 \pmod{4} \), there are three solutions modulo \( p^k \).
(ii) for \( p \equiv 3 \pmod{4} \), there is one solution modulo \( p^k \).

**Esercizio 6.** Let \( P(x) \in \mathbb{Z}/p\mathbb{Z}[x] \) be a polynomial of degree \( d \). Prove that \( P(x) \) has \( d \) distinct roots in \( \mathbb{Z}/p\mathbb{Z} \) if and only if \( P(x) \) divides \( x^p - x \), namely
\[ x^p - x \equiv P(x)Q(x) \pmod{p} \]

for some polynomial \( Q(x) \in \mathbb{Z}/p\mathbb{Z}[x] \).
Solution
If \( P(x) \) has \( d \) distinct solutions, say \( \alpha_1, \ldots, \alpha_d \), then by dividing by \( x - \alpha_i \) repeatedly, we immediately get that it must be
\[
P(x) \equiv a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_d) \mod (p)
\]
Therefore, since \( x^p - x = (x - 0)(x - 1)(x - 2) \ldots (x - p + 1) \), we can just take
\[
Q(x) = [a_0]^{-1}(x - \beta_1)(x - \beta_2) \ldots (x - \beta_{p-d}) \mod (p)
\]
where \( \{\beta_1, \ldots, \beta_{p-d}\} = \{0,1, \ldots, p-1\}\setminus\{\alpha_1, \ldots, \alpha_d\} \).

Conversely, suppose that \( x^p - x = P(x)Q(x) \). Then, \( Q \) must have degree \( p - d \). Moreover, each of the numbers 0,1,\ldots, p-1, being a root of \( x^p - x \), must be a root of \( P(x) \) or \( Q(x) \). Which implies that \( P(x) \) must have \( d \) roots and \( Q(x) \) must have \( p - d \) roots (modulo \( p \)).