Problem 1. 1. For which positive integers $m$ do we have $101 \equiv 1 \mod m$?

2. Does the equation $23x + 57y = 1$ have a solution $(x, y) \in \mathbb{Z}^2$? Justify.

3. Does the equation $23x - 57y = 6$ have a solution $(x, y) \in \mathbb{Z}^2$? Justify.

4. Does the equation $105x + 25y = 47$ have a solution $(x, y) \in \mathbb{Z}^2$? Justify.

5. Decompose the polynomial $X^2 - X - 2$ as a product of two polynomials with degree 1.


9. Use the Euclidean algorithm to find the gcd of 17 and 125.

10. What is the last digit of $7^{143}$?

Solution 1. 1. You need to list here all the divisors of 100.

2. The equation has a solution because 23 and 57 are relatively prime.

3. The equation has a solution: let $(u, v)$ be a solution to $23u + 57v = 1$. Then $(x, y) = (6u, -6v)$ is a solution to $23x - 57y = 6$.

4. If there was $(x, y) \in \mathbb{Z}^2$ such that $105x + 25y = 5(21x + 5y) = 47$, then 5 would divide 47. Contradiction. So this equation has no solution.

5. $X^2 - X - 2 = (X + 1)(X - 2)$.

6. The discriminant of $X^2 - X - 1$ is 5 so the roots of $X^2 - X - 1$ are

$$\frac{1 - \sqrt{5}}{2} \text{ and } \frac{1 + \sqrt{5}}{2}$$

and

$$X^2 - X - 1 = (X - \frac{1 - \sqrt{5}}{2})(X - \frac{1 + \sqrt{5}}{2})$$

is not irreducible in $\mathbb{R}[X]$.

7. Since $\sqrt{5} \not\in \mathbb{Q}$, the previous decomposition is not a decomposition in $\mathbb{Q}[X]$ and $X^2 - X - 1$ is irreducible in $\mathbb{Q}[X]$.

8. Proceed to the division of $X^3 + X^2 + 2X + 1$ by $X^2 + X + 1$ and obtain $X^3 + X^2 + 2X + 1 = X(X^2 + X + 1) + (X + 1)$. So if $X^2 + X + 1$ divided $X^3 + X^2 + 2X + 1$, it would also divide $X^3 + X^2 + 2X + 1 - X(X^2 + X + 1) = X + 1$ which is a contradiction.
9. \[ 125 = 17 \times 7 + 6 \]
\[ 17 = 6 \times 2 + 5 \]
\[ 6 = 5 \times 1 + 1 \]
The last remainder being 1, we have proved that 125 and 17 are coprime.

10. We have \[ 7^2 \equiv 9 \mod 10, \ 7^3 \equiv 7 \times 9 \equiv 3 \mod 10, \ 7^4 \equiv 7 \times 3 \equiv 1 \mod 10. \] We have \[ 143 = 4 \times 35 + 3 \] so
\[ 7^{143} = (7^4)^{35} \times 7^3 \equiv 7^2 \equiv 3 \mod 10. \]

**Problem 2.**

1. Prove the following result: for \( a, b, c \in \mathbb{Z} - \{0\} \) such that \( \gcd(a, b) = 1 \), if \( a \) divides \( bc \) then \( a \) divides \( c \).

2. Use the Euclidean algorithm to find \((u_0, v_0) \in \mathbb{Z}^2\) such that
\[ 281u_0 + 156v_0 = 1. \]

3. Let \((u, v) \in \mathbb{Z}^2\) be another solution to this equation: we have \[ 281u + 156v = 1. \]
   
   (a) Prove that there is \( k \in \mathbb{Z} \) such that \( v = v_0 + 281k \).
   
   (b) Give the expression of \( u \) as a function of \( u_0 \) and \( k \).
   
   (c) Give two new solutions \((u_1, v_1)\) and \((u_2, v_2)\) to the equation we are considering.

**Solution 2.**

1. See your notes or the book.

2. \[ 281 = 156 \times 1 + 125 \]
\[ 156 = 125 \times 1 + 31 \]
\[ 125 = 31 \times 4 + 1. \]

Then:
\[ 1 = 125 - 31 \times 4 \]
\[ 1 = 125 - 4 \times (156 - 125) = 5 \times 125 - 4 \times 156. \]
\[ 1 = 5 \times (281 - 156) - 4 \times 156 = 5 \times 281 - 9 \times 156. \] so
\[ u_0 = 5, \ v_0 = -9. \]

3. Let \((u, v) \in \mathbb{Z}^2\) be another solution to this equation.
   
   (a) We have \[ 281u + 156v = 281u_0 + 156v_0 \] so \[ 281(u_0 - u) = 156(v - v_0). \] In particular, we see that 281 divides \( 156(v - v_0) \). But we just saw that 281 and 156 are relatively prime, therefore 281 divides \( v - v_0 \) and there is \( k \in \mathbb{Z} \) such that \( v = v_0 + 281k \).
   
   (b) Plug in \( v = v_0 + 281k \) into the equation \[ 281(u_0 - u) = 156(v - v_0). \] We get \( u = u_0 - 156k \).
(c) For example, with $k = 1$ and $k = -1$:

$$(u_1, v_1) = (5 - 156, -9 + 281)$$ and $$(u_2, v_2) = (5 + 156, -9 - 281).$$

**Problem 3.**

1. Let $m \in \mathbb{N}$. Prove that $8$ divides $m(m + 1)(m + 2)(m + 3)$. *(You can split into cases depending on the value of $m \mod 8$).*

2. Let $n \in \mathbb{N}$, $n \geq 1$.

   (a) Prove that $(5n + 5)!$ is a product of $5(n + 1)$ by a multiple of $8$.

   (b) Prove by induction that $40^n n!$ divides $(5n)!$.

**Solution 3.**

1. Let $m \in \mathbb{N}$.

   If $m \equiv 0 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv 0 \times 1 \times 2 \times 3 \equiv 0 \mod 8$.

   If $m \equiv 1 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv 1 \times 2 \times 3 \times 4 \equiv 0 \mod 8$.

   If $m \equiv 2 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv 2 \times 3 \times 4 \times 5 \equiv 0 \mod 8$.

   If $m \equiv 3 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv 3 \times 4 \times 5 \times 6 \equiv 0 \mod 8$.

   If $m \equiv 4 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv 4 \times 5 \times 6 \times 7 \equiv 0 \mod 8$.

   If $m \equiv 5 \equiv -3 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv (-3) \times (-2) \times (-1) \times 0 \equiv 0 \mod 8$.

   If $m \equiv 6 \equiv -2 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv (-2) \times (-1) \times 0 \times 1 \equiv 0 \mod 8$.

   If $m \equiv 7 \equiv -1 \mod 8$, then $m(m + 1)(m + 2)(m + 3) \equiv (-1) \times 0 \times 1 \times 2 \equiv 0 \mod 8$.

   So in any case $m(m + 1)(m + 2)(m + 3) \equiv 0 \mod 8$.

2. Let $n \in \mathbb{N}$, $n \geq 1$.

   (a) We have $(5n + 5)! = (5(n + 1))((5n + 4)(5n + 3)(5n + 2)(5n + 1))(5n)!$. Set $M = (5n + 4)(5n + 3)(5n + 2)(5n + 1)$. It is a product of 4 consecutive numbers so it is a multiple of 8. Therefore there is $k \in \mathbb{N}$ such that

   $$(5n + 5)! = (5(n + 1))8k(5n)! = 40k \times (n + 1)(5n)!.$$  

   (b) Let us prove by induction on $n \geq 1$ that $40^n n!$ divides $(5n)!$:

      Base step: for $n = 1$ we have $40^1 n! = 40$ and $5! = 120$ and $40$ divides $120$.

      Induction step: suppose that $40^n n_0!$ divides $(5n_0)!$ for some $n_0 \geq 1$. Now consider $(5(n_0 + 1))!$. By the previous question, there is $k \in \mathbb{N}$ such that

      $$(5(n_0 + 1))! = 40k \times (n_0 + 1)(5n_0)!. $$
By induction hypothesis, there is \( \ell \in \mathbb{N} \) such that \((5n_0)! = \ell \times 40^{n_0} n_0! \) so
\[(5(n_0 + 1))! = 40k \times (n_0 + 1)\ell \times 40^{n_0} n_0! = k \times \ell \times 40^{n_0+1}(n_0 + 1)!\]
which proves that \(40^{n_0+1}(n_0 + 1)!\) divides \((5(n_0 + 1))!\).

**Problem 4.** We define the sequence \((u_n)_{n \in \mathbb{N}}\) by
\[u_n = (3 - \sqrt{5})^n + (3 + \sqrt{5})^n.\]

1. Let \( n \in \mathbb{N} \). Compute \( u_{n+2} - 6u_{n+1} + 4u_n \).
2. Prove by double induction that \( u_n \) is an integer which is divisible by \( 2^n \) for any \( n \in \mathbb{N} \).

**Solution 4.**

1. Let \( n \in \mathbb{N} \). We have
\[
u_{n+2} - 6u_{n+1} + 4u_n = (3 - \sqrt{5})^{n+2} - 6(3 - \sqrt{5})^{n+1} + 4(3 - \sqrt{5})^n
+ (3 + \sqrt{5})^{n+2} - 6(3 + \sqrt{5})^{n+1} + 4(3 + \sqrt{5})^n
= (3 - \sqrt{5})^n[(3 - \sqrt{5})^2 - 6(3 - \sqrt{5}) + 4]
+ (3 + \sqrt{5})^n[(3 + \sqrt{5})^2 - 6(3 + \sqrt{5}) + 4]
= (3 - \sqrt{5})^n[9 - 6\sqrt{5} + 5 - 18 + 6\sqrt{5} + 4]
+ (3 + \sqrt{5})^n[9 + 6\sqrt{5} + 5 - 18 - 6\sqrt{5} + 4]
= 0
\]

2. We prove by double induction that \( u_n \) is an integer which is divisible by \( 2^n \) for any \( n \in \mathbb{N} \).

Base step: For \( n = 0 \) we have \( u_0 = 1 \): it is an integer which is divisible by \( 2^0 = 1 \). For \( n = 1 \) we have \( u_1 = 6 \): it is an integer which is divisible by \( 2^1 = 2 \).

Induction step: suppose that \( u_{n_0} \) is an integer which is divisible by \( 2^{n_0} \) and \( u_{n_0+1} \) is an integer which is divisible by \( 2^{n_0+1} \) for some \( n_0 \geq 0 \). Now consider \( u_{n_0+2} \). By the previous question, \( u_{n_0+2} = 6u_{n_0+1} - 4u_{n_0} \). By induction hypothesis, \( u_{n_0} \) and \( u_{n_0+1} \) are integers so \( u_{n_0+2} \) is also an integer. Moreover, there is \( k \in \mathbb{Z} \) and \( \ell \in \mathbb{Z} \) such that \( u_{n_0} = k \times 2^{n_0} \) and \( u_{n_0+1} = \ell \times 2^{n_0+1} \). Therefore,
\[
u_{n_0+2} = 6\ell \times 2^{n_0+1} - 4k \times 2^{n_0} = 3\ell \times 2^{n_0+2} - k \times 2^{n_0+2}
\]
so \( u_{n_0+2} \) is divisible by \( 2^{n_0+2} \).