**Instructions.** Answer each of the questions on your own paper, and be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. **[18 Points]** Prove by induction that for all positive integers \( n \),
   \[
   \sum_{i=1}^{n} i(i - 1) = \frac{(n - 1)n(n + 1)}{3}
   \]

   **Solution.** Let \( P(n) \) be the statement:
   
   \( (*_n) \quad \sum_{i=1}^{n} i(i - 1) = \frac{(n - 1)n(n + 1)}{3} \).
   
   The problem is to prove by induction that \( P(n) \) is a true statement for all integers \( n \geq 1 \).

   **Base case:** If \( n = 1 \), \( P(1) \) is the statement
   \[
   \sum_{i=1}^{1} i(i - 1) = \frac{(1 - 1)1(1 + 1)}{3}.
   \]
   Since both the left hand side and right hand side evaluate to 0, \( P(1) \) is a true statement.

   **Induction step:** Suppose that \( k \geq 1 \) and that \( P(k) \) is a true statement. That is assume
   
   \( (*_k) \quad \sum_{i=1}^{k} i(i - 1) = \frac{(k - 1)k(k + 1)}{3} \).
   
   It must then be shown, under this assumption, that the statement \( P(k+1) \) is also true. That is, we must show that the validity of equation \( (*_k) \) implies the validity of equation \( (*_{k+1}) \):
   
   \( (*_{k+1}) \quad \sum_{i=1}^{k+1} i(i - 1) = \frac{((k + 1) - 1)(k + 1)((k + 1) + 1)}{3} = \frac{k(k+1)(k+2)}{3} \).
   
   To see this implication, we argue as follows.
   
   \[
   \sum_{i=1}^{k+1} i(i - 1) = \sum_{i=1}^{k} i(i - 1) + (k + 1)k
   = \frac{(k - 1)k(k + 1)}{3} + (k + 1)k \text{ using } (*_k)
   = \frac{(k - 1)k(k + 1) + 3(k + 1)k}{3}
   = \frac{(k - 1)k(k + 1) + 3(k + 1)k}{3}
   = \frac{k(k + 1)((k - 1) + 3)}{3}
   = \frac{k(k + 1)(k+2)}{3}.
   \]
Thus, we have shown that if \((\ast_k)\) is a valid equality, then so is \((\ast_{k+1})\). That is, the truth of \(P(k)\) implies the truth of \(P(k + 1)\), and the inductive step is verified.

Since both the base step and the inductive step have been established, it follows from the principle of mathematical induction that \(P(n)\) is true for all \(n \geq 1\). ▶

2. [16 Points]

(a) Compute the greatest common divisor \(d = (1776, 1492)\) of the integers 1776 and 1492, and write \(d\) in the form \(d = 1776 \cdot s + 1492 \cdot t\).

▶ Solution. Use the matrix method for the Euclidean algorithm:

\[
\begin{bmatrix}
1 & 0 & 1492 \\
0 & 1 & 1776
\end{bmatrix}
\rightarrow
\begin{bmatrix}
1 & 0 & 1492 \\
-1 & 1 & 284
\end{bmatrix}
\rightarrow
\begin{bmatrix}
6 & -5 & 72 \\
-1 & 1 & 284
\end{bmatrix}
\rightarrow
\begin{bmatrix}
6 & -5 & 72 \\
-19 & 16 & 68
\end{bmatrix}
\rightarrow
\begin{bmatrix}
25 & -21 & 4 \\
-19 & 16 & 68
\end{bmatrix}
\]

Since \(4 \mid 68\), it follows that \(4 = (1776, 1492)\) and the first row of the last matrix gives the equation

\[4 = 25 \cdot 1492 - 21 \cdot 1776.\]
▶

(b) Compute the least common multiple \(m = [1776, 1492]\).

▶ Solution. \([1776, 1492] = \frac{1776 \cdot 1492}{4} = 662448.\)
▶

3. [16 Points] Assume that \(a\) is an integer with \((a, 72) = 6\) and \((a, 245) = 7\) (some examples of integers \(a\) with these properties are 42, 462, and 546), and let \(b = 3^4 \cdot 5^3 \cdot 7^3\).

(a) Write the prime factorization for each of the integers 72 and 245.

▶ Solution. \(72 = 2^3 \cdot 3^2; 245 = 5 \cdot 7^2.\)
▶

(b) For \(p\) each of the primes 2, 3, 5, and 7, determine the highest power of \(p\) which divides \(a\), and using this information determine the greatest common divisor \((a, b)\).

▶ Solution. From \((a, 72) = 6 = 2^1 \cdot 3^1\), we conclude that 2 and 3 divide \(a\) to at least power 1, and since \(2^2 \nmid 72\) and \(3^3 \nmid 72\), it follows that 1 is the highest power of 2 or 3 to divide \(a\). Otherwise \((a, 72)\) would have higher powers of 2 or 3. Similarly, \((a, 245) = 7\) and \(245 = 5 \cdot 7^2\) means that 5 \(\nmid a\) and 7 \(\nmid a\), but \(7^2 \nmid a\). Hence, 2, 3, and 7 divide \(a\) to the first power, and 5 does not divide \(a\). Thus \(a = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot m\) where \(m\) is not divisible by 2, 3, 5, or 7. Hence \((a, b) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 = 21.\)
▶

(c) What is the highest power of \(7\) which divides the least common multiple \([a, b]?\)
4. [16 Points] This exercise makes use of the following equation:

\[ 1 = 13 \cdot 101 - 41 \cdot 32. \]

Using this equation (i.e., it is not necessary to use the Euclidean algorithm to recreate it), answer the following questions.

(a) Compute the multiplicative inverse of 32 in \( \mathbb{Z}_{101} \).

▶ Solution. \( [32]_{101}^{-1} = [−41]_{101} = [60]_{101}. \)

(b) Solve the congruence equation \( 32x \equiv 3 \mod 101. \)

▶ Solution. In terms of congruence classes:

\[ [x]_{101} = [32]_{101}^{-1} [3]_{101} = [60]_{101} [3]_{101} = [180]_{101} = [79]_{101}. \]

In terms of integers: \( x = 79 + 101k \) where \( k \) is an arbitrary integer.

5. [16 Points] This problem concerns arithmetic modulo 18. All answers should only involve expressions of the form \([a]_{18}\) with \( a \) an integer satisfying \( 0 \leq a < 18 \).

(a) Compute \([9]_{18} + [16]_{18}\). Answer. \([7]_{18}\).

(b) Compute \([9]_{18}[16]_{18}\). Answer. \([0]_{18}\).

(c) Compute \([5]_{18}^{-1}\). Answer. \([11]_{18}\) since \( 11 \cdot 5 - 3 \cdot 18 = 1 \).

(d) List the invertible elements of \( \mathbb{Z}_{18} \).

▶ Solution. The invertible elements of \( \mathbb{Z}_{18} \) are the congruence class \([a]_{18}\) such that \((a, 18) = 1\). Hence \( \mathbb{G}_{18} = \mathbb{Z}_{18}^* = \{[1]_{18}, [5]_{18}, [7]_{18}, [11]_{18}, [13]_{18}, [17]_{18}\}. \)

(e) List the zero divisors of \( \mathbb{Z}_{18} \).

▶ Solution. The zero divisors of \( \mathbb{Z}_{18} \) are precisely the nonzero congruence classes that are not invertible. Hence, the set of zero divisors is


6. [18 Points] Solve the system of simultaneous linear congruences:

\[ x \equiv 4 \mod 24 \]
\[ x \equiv 7 \mod 11 \]

▶ Solution. Apply the Euclidean algorithm, or simply observe that the equation \( 1 = 11 \cdot 11 - 5 \cdot 24 \) holds. Since \( 11 \cdot 24 = 264 \), it follows that \( x \equiv 4 \cdot 11 \cdot 11 - 7 \cdot 5 \cdot 24 = -356 \equiv 172 \mod 264 \). This means that \( x = 172 + k \cdot 264 \) where \( k \) is an arbitrary integer.