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. [**15 Points**] Let $m = 715$ and $n = 546$.

   (a) Calculate the greatest common divisor $d = \gcd(m,\, n)$.

   ▶ **Solution.** Apply the Euclidean Algorithm:

$$\begin{aligned} 715 &= 1 \cdot 546 + 169 \\ 546 &= 3 \cdot 169 + 39 \\ 169 &= 4 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 + 0 \end{aligned}$$

   Thus, $d = \gcd(715,\, 546) = 13$. ◀

   (b) Write d in the form $sm + tn$ for some integers s and t.

   ▶ **Solution.** Reverse the above calculations to write d as a linear combination:

$$\begin{aligned} 13 &= 169 - 4 \cdot 39 \\ &= 169 - 4(546 - 3 \cdot 169) = 13 \cdot 169 - 4 \cdot 546 \\ &= 13(715 - 546) - 4 \cdot 546 = 13 \cdot 715 - 17 \cdot 546. \end{aligned}$$

   Thus $13 = 13 \cdot 715 - 17 \cdot 546$. ◀

   (c) Calculate the least common multiple $\operatorname{lcm}(m,\, n)$.

   ▶ **Solution.**

$$\operatorname{lcm}(715,\, 546) = \frac{715 \cdot 546}{\gcd(715,\, 546)} = \frac{390390}{13} = 30030.$$

   ◀

2. [**20 Points**] Use induction to prove that the equation

$$\sum_{k=1}^{n} (4k - 1) = 2n^2 + n$$

is valid for all integers $n \geq 1$. Note that expanding the summation, the equation is

$$3 + 7 + 11 + \cdots + (4n - 1) = 2n^2 + n.$$

▶ **Solution.** Let $P(n)$ be the statement "$1 + 3 + 5 + \cdots + (4n - 1) = 2n^2 + n$". Then $P(1)$ is the statement "$3 = 1^2 + 1$", which is true. Now assume that $P(k)$ is true. That is , assume that "$1 + 3 + 5 + \cdots + (4k - 1) = 2k^2 + k$". Then,

$$\begin{aligned} 1 + 3 + 5 + \cdots + (4k - 1) + (4(k + 1) - 1) &= 2k^2 + k + (4(k + 1) - 1) \\ &= 2k^2 + 5k + 3 = 2k^2 + 4k + 2 + k + 1 \\ &= 2(k + 1)^2 + (k + 1) \end{aligned}$$

Therefore, whenever $P(k)$ is true, $P(k + 1)$ is also true. By the induction principle, $P(n)$ is thus true for all $n \geq 1$. ◀

3. [**15 Points**] Let $A \xrightarrow{\alpha} B \xrightarrow{\beta} A$ satisfy $\beta\alpha = 1_A$.

   (a) Show that β is onto.

   ▶ **Solution.** Let $a \in A$. Then $a = 1_A(a) = \beta\alpha(a) = \beta(\alpha(a))$. Thus $a = \beta(b)$ for $b = \alpha(a)$, so β is onto. ◀

   (b) Give an example for which β does not have an inverse.

   ▶ **Solution.** Let $A = \{0\}$, $B = \{1, 2\}$, $\alpha : A \to B$ is defined by $\alpha(0) = 1$, and $\beta : B \to A$ is defined by $\beta(1) = 0$, $\beta(2) = 0$. Then, $\beta\alpha(0) = \beta(\alpha(0)) = \beta(1) = 0 = 1_A(0)$, and hence $\beta\alpha = 1_A$. However, β is not injective, so it cannot have an inverse. ◀

4. [**20 Points**] This exercise makes use of the following equation:

$$1 = 6 \cdot 111 - 19 \cdot 35.$$

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

   (a) Compute the multiplicative inverse of $\overline{35}$ in $\mathbb{Z}_{111}$. Express your answer in the standard form $\overline{a}$ where $0 \leq a < 111$.

   ▶ **Solution.** From the given equation, the multiplicative inverse of $\overline{35}$ is

$$\overline{-19} = \overline{92} \in \mathbb{Z}_{111}.$$

◀

   (b) Solve the equation $\overline{35}x = \overline{9}$ in $\mathbb{Z}_{111}$. Express your answer in the standard form $x = \overline{b}$ where $0 \leq b < 111$.

   ▶ **Solution.** $x = \left(\overline{35}\right)^{-1} \cdot \overline{9} = \overline{92} \cdot \overline{9} = \overline{828} = \overline{51}$ since $828 = 7 \cdot 111 + 51$. ◀

   (c) Find the smallest positive solution of the system of simultaneous linear congruences:

$$\begin{aligned} x &\equiv 6 \pmod{111} \\ x &\equiv 5 \pmod{19}. \end{aligned}$$

   ▶ **Solution.** The solutions are $x = 6(-19 \cdot 35) + 5(6 \cdot 111) = -660 \pmod{(111 \cdot 19)}$. The smallest positive solution is thus $x = -660 + 111 \cdot 19 = -660 + 2109 = 1449$. ◀

5. [**15 Points**] Let $A = \mathbb{R} \times \mathbb{R}$ and define a relation $\equiv$ on A by $(a, b) \equiv (a_1\, b_1)$ if $a^2 + b^2 = a_1^2 + b_1^2$.

   (a) Verify that $\equiv$ is an equivalence relation on A.

   ▶ **Solution.** It is necessary to verify that the relation is (1) reflexive, (2) symmetric, and (3) transitive.

   Reflexive: $(a, b) \equiv (a, b)$ for all $(a, b) \in A$ since $a^2 + b^2 = a^2 + b^2$, so the relation is reflexive.

   Symmetric: If $(a, b) \equiv (a_1, b_1)$ then $a^2 + b^2 = a_1^2 + b_1^2$. Then, by the symmetry of equality, $a_1^2 + b_1^2 = a^2 + b^2$ so $(a_1, b_1) \equiv (a, b)$. Hence, $\equiv$ is symmetric.

Transitive: If $(a,\, b) \equiv (a_1,\, b_1)$ and $(a_1,\, b_1) \equiv (a_2,\, b_2)$ then $a^2 + b^2 = a_1^2 + b_1^2$ and $a_1^2 + b_1^2 = a_2^2 + b_2^2$. By the transitivity of equality, it follows that $a^2 + b^2 = a_2^2 + b_2^2$ and hence $(a,\, b) \equiv (a_2,\, b_2)$. Thus $\equiv$ is transitive.

Since $\equiv$ is reflexive, symmetric, and transitive, it is an equivalence relation.

You can also show that $\equiv$ is an equivalence relation by observing that $\equiv$ is the kernel equivalence (Example 4, page 18) of the mapping $\alpha : A \to \mathbb{R}$ defined by $\alpha(a,\, b) = a^2 + b^2$. ◀

(b) Find the equivalence class $[(1,\, 0)]$.

▶ **Solution.** $[(1,\, 0)] = \left\{(a,\, b) \in A \mid a^2 + b^2 = 1^1 + 0^2 = 1\right\}$. That is $[(1,\, 0)]$ is the circle of radius 1 centered at the origin $(0,\, 0)$. ◀

(c) More generally, for each $(a,\, b) \in \mathbb{R} \times \mathbb{R}$, give a simple geometric description of the equivalence class $[(a,\, b)]$.

▶ **Solution.** The equivalence class $[(a,\, b)]$ is the circle of radius $r = \sqrt{a^2 + b^2}$ centered at the origin $(0,\, 0)$. That is,

$$[(a,\, b)] = \left\{(x,\, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = r^2\right\}.$$

◀

6. **[20 Points]** Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 3 & 2 & 7 & 6 & 1 & 5 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 7 & 8 & 1 & 6 & 4 \end{pmatrix}$.

(a) Write σ as a product of disjoint cycles.

▶ **Solution.** $\sigma = \begin{pmatrix} 1 & 8 & 5 & 7 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$ ◀

(b) Write σ as a product of transpositions. Recall that a transposition is a 2-cycle.

▶ **Solution.** From the cycle decomposition in part (a):

$$\sigma = \begin{pmatrix} 1 & 8 \end{pmatrix} \begin{pmatrix} 8 & 5 \end{pmatrix} \begin{pmatrix} 5 & 7 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$$

◀

(c) Compute $\sigma\tau$ and $\tau\sigma$.

▶ **Solution.** $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 5 & 8 & 6 & 2 \end{pmatrix}$ and $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 2 & 5 & 6 & 1 & 3 & 8 \end{pmatrix}$. ◀