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]**

   (a) Calculate the greatest common divisor $d = (378, 490)$ by the Euclidean algorithm, and write d in the form $378 \cdot s + 490 \cdot t$ for some integers s and t.

   ▶ **Solution.** Use the matrix method:

   $$\begin{bmatrix} 1 & 0 & 378 \\ 0 & 1 & 490 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 378 \\ -1 & 1 & 112 \end{bmatrix} \quad \begin{bmatrix} 4 & -3 & 42 \\ -1 & 1 & 112 \end{bmatrix} \quad \begin{bmatrix} 4 & -3 & 42 \\ -9 & 7 & 28 \end{bmatrix} \quad \begin{bmatrix} 13 & -10 & 14 \\ -9 & 7 & 28 \end{bmatrix}.$$

   Hence, $(378, 490) = 14$, and the first line of the last matrix gives

   $$14 = 13 \cdot 378 = 10 \cdot 490.$$

   ◀

   (b) Calculate $[378, 490]$.

   ▶ **Solution.**

   $$[378, 490] = \frac{378 \cdot 490}{(378, 490)} = \frac{378 \cdot 490}{14} = 13,230.$$

   ◀

   (c) Describe all of the integers n that can be written in the form $n = 378 \cdot u + 490 \cdot v$ for some integers u and v. That is, identify the set S in the equation $378\mathbb{Z} + 490\mathbb{Z} = S$.

   ▶ **Solution.** By Theorem 1.1.6, $S = 14\mathbb{Z}$. That is, S is the set of all multiples of the greatest common divisor of 378 and 490. ◀

2. **[20 Points]** This exercise makes use of the following equation:

   $$1 = 7 \cdot 103 - 48 \cdot 15.$$

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

   (a) Compute the multiplicative inverse of $[15]_{103}$ in $\mathbb{Z}_{103}$. Express your answer in the standard form $[b]_{103}$ where $0 \leq b < 103$.

   ▶ **Solution.** $[15]_{103} = [-48]_{103} = [55]_{103}$. ◀

   (b) Solve the congruence equation $15x \equiv 8 \pmod{103}$. Express your answer in the standard form $x \equiv b \pmod{103}$ where $0 \leq b < 103$.

   ▶ **Solution.** Multiply the given equation by 8 to get

   $$8 = 8 \cdot 7 \cdot 103 - 8 \cdot 48 \cdot 15.$$

   This equation means that $x = -8 \cdot 48$ satisfies $15x \equiv 8 \pmod{103}$. Thus, $x = -8 \cdot 48 = -384 \equiv 28 \pmod{103}$. ◀

(c) Solve the system of simultaneous linear congruences:

$$\begin{aligned} x &\equiv 8 \pmod{103} \\ x &\equiv 3 \pmod{48}. \end{aligned}$$

Give your answer in for form $x \equiv r \pmod{m}$ where r is the smallest possible *positive* integer and m is determined from the problem.

► **Solution.**

$$\begin{aligned} x &\equiv 8 \cdot (-48 \cdot 15) + 3 \cdot (7 \cdot 103) \pmod{103 \cdot 48} \\ &\equiv -3597 \pmod{4944} \\ &\equiv 1347 \pmod{4944}. \end{aligned}$$

◄

3. **[20 Points]** This problem concerns arithmetic modulo 21. All answers should be expressed in the standard form $[a]_{21}$ with a an integer satisfying $0 \leq a < 21$.

(a) Compute $[9]_{21} + [16]_{21}$.

► **Solution.** $[9]_{21} + [16]_{21} = [25]_{21} = [4]_{21}$. ◄

(b) Compute $[9]_{21}[16]_{21}$.

► **Solution.** $[9]_{21}[16]_{21} = [144]_{21} = [18]_{21}$. ◄

(c) Compute $[5]_{21}^{-1}$.

► **Solution.** By the Euclidean algorithm or trial and error: $5 \cdot 17 = 85 = 4 \cdot 21 + 1$. Hence $[5]_{21}^{-1} = [17]_{21}$. ◄

(d) Find a nonzero $[b]_{21}$ such that $[12]_{21}[b]_{21} = [0]_{21}$.

► **Solution.** $7 \cdot 12 = 84 = 4 \cdot 21$ so $[12]_{21}[7]_{21} = [84]_{21} = [0]_{21}$ and $[7]_{21} \neq [0]_{21}$. ◄

(e) List the invertible elements of $\mathbb{Z}_{21}$.

► **Solution.** $[a]_{21}$ is invertible if and only if $(a, 21) = 1$, that is, if and only if a is not divisible by either 3 or 7. Hence the invertible elements are

$$\mathbb{Z}_{21}^* = \{[1]_{21}, [2]_{21}, [4]_{21}, [5]_{21}, [8]_{21}, [10]_{21}, [11]_{21}, [13]_{21}, [16]_{21}, [17]_{21}, [19]_{21}, [20]_{21}\}.$$

◄

(f) List the zero divisors of $\mathbb{Z}_{21}$.

► **Solution.** The zero divisors are the elements of $\mathbb{Z}_{21}$ that are not invertible. Hence, these are the set

$$\{[0]_{21}, [3]_{21}, [6]_{21}, [7]_{21}, [9]_{21}, [12]_{21}, [14]_{21}, [15]_{21}, [18]_{21}\}$$

◄

4. **[18 Points]**

   (a) If a and b are integers, write the definition of the statement "a divides b". Be sure to write in a complete sentence.

   ▶ **Solution.** If a and b are integers, then a divides b provided that there is an integer q such that $b = aq$. ◀

   (b) If a, b, and c are integers such that $a|b$ and $a|(b+c)$, then prove, directly from the definition of divides (which you have conveniently provided in Part (a)), that $a|c$.

   ▶ **Solution.** Since $a|b$ there is an integer q with $b = aq$ and since $a|(b+c)$ there is an integer q' with $b + c = aq'$. Then

   $$c = (b+c) - b = aq' - aq = a(q' - q).$$

   Since $\mathbb{Z}$ is closed under subtraction, it follows that $q' - q = m$ is an integer. Hence, $c = am$, where m is an integer, so that $a|c$. ◀

5. **[12 Points]** Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.

   (a) Fill in the box with an appropriate statement about a and b to provide a true result:

   If $b|ac$ *and* $\boxed{(a,b) = 1}$, *then* $b|c$.

   (b) Provide an example of integers a, b, c for which $b|ac$, but $b \nmid c$. Naturally, the condition you listed in part (a) will not be satisfied.

   ▶ **Solution.** $6|2 \cdot 3$ but $6 \nmid 2$ and $6 \nmid 3$. ◀

6. **[12 Points]** For each of the following relations on the real numbers $\mathbb{R}$, determine which of the properties (i) reflexive, (ii) symmetric, and (iii) transitive hold.

   (a) For $a, b \in \mathbb{R}$, define $a \sim b$ if $a \leq b$.

   ▶ **Solution.** $a \sim a$ for all $a \in \mathbb{R}$ since $a \leq a$ for all $a \in \mathbb{R}$.
   If $a \sim b$ and $b \sim c$ then $a \leq b$ and $b \leq c$. Hence, by transitivity of $\leq$, $a \leq c$ and hence $a \sim c$.
   $1 \sim 2$ since $1 \leq 2$, but $2 \not\leq 1$ so $2 \nsim 1$.
   Therefore the relation $\sim$ is reflexive and transitive, but not symmetric. ◀

   (b) For $a, b \in \mathbb{R}$, define $a \sim b$ if $|a - b| \leq 1$.

   ▶ **Solution.** $a \sim a$ for all $a \in \mathbb{R}$ since $|a - a| = 0 \leq 1$ for all $a \in \mathbb{R}$.
   If $a \sim b$, then $|a - b| \leq 1$. But then $|b - a| = |-(b - a)| = |a - b| \leq 1$ and hence, $b \sim a$.
   $0 \sim 1$ since $|0 - 1| = 1 \leq 1$ and $1 \sim 2$ since $|1 - 2| = 1 \leq 1$, but $0 \nsim 2$ since $|0 - 2| = 2 \not\leq 1$.
   Therefore the relation $\sim$ is reflexive and symmetric, but not transitive. ◀

   Are either of these relations an equivalence relation?