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]

   (a) Find the quotient q and remainder r when 525 is divided by 231.

   ▶ **Solution.** $525 = 2 \cdot 231 + 63$ so $q = 2$ and $r = 63$. ◀

   (b) Calculate the greatest common divisor $d = (525,\ 231)$ by the Euclidean algorithm.

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

$$\begin{bmatrix} 1 & 0 & 525 \\ 0 & 1 & 231 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -2 & 63 \\ 0 & 1 & 231 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -2 & 63 \\ -3 & 7 & 42 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 4 & -9 & 21 \\ -3 & 7 & 42 \end{bmatrix}.$$

   Hence, $(525,\ 231) = 21$. ◀

   (c) Using Part (b), write d in the form $s \cdot 525 + t \cdot 231$ for some integers s and t.

   ▶ **Solution.** From the first row of the last matrix in Part (b), $21 = 4 \cdot 525_{(} -9) \cdot 231$. ◀

2. [14 Points]

   (a) Find all solutions to the congruence $32x \equiv 7 \mod 101$. The identity

$$1 = 13 \cdot 101 - 41 \cdot 32,$$

   which may be useful, can be assumed.

   ▶ **Solution.** From the given equation, $(-41) \cdot 32 \equiv 1 \pmod{101}$ so that

$$x \equiv (-41)32x \equiv (-41)7 \equiv -287 \equiv 16 \pmod{101}.$$

   ◀

   (b) Among the solutions found in Part (a), determine the unique solution x with $0 \leq x \leq 100$.

   ▶ **Solution.** The only solution in this range is $x = 16$. ◀

3. [20 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 we say that a divides b if $b = aq$ for some integer q. ◀

   (b) If a, b, and c are integers such that $a|b$ and $2a + c = 3b$, then prove, directly from the definition of divides (which you have conveniently provided in Part (a)), that $a|c$.

▶ **Solution.** Assume that $a|b$ and that $2a + c = 3b$. Then $b = aq$ (since $a|b$) so that $c = 3b - 2a = 3(aq) - 2a = a(3q - 2) = au$ where $u = 3q - 2$ is an integer since q is an integer and the integers are closed under multiplication and subtraction. Thus, $a|c$ ◀

4. [20 Points]

(a) Complete the following statement of Euclid's Lemma: *If p is a prime and a and b are integers such that $p|ab$, then* $\boxed{p|a \text{ or } p|b.}$

(b) Let a and b be integers. Prove that if $5|ab$, then $25|a^2$ or $25|b^2$.

▶ **Solution.** If $5|ab$ then by Euclid's lemma, $5|a$ or $5|b$. In case $5|a$ we have that $a = 5k$ for some $k \in \mathbb{Z}$. Hence $a^2 = 25k^2$ and k^2 is an integer, so $25|a^2$. In case $5|b$, the same argument shows that $25|b^2$. ◀

5. [15 Points] The observation that $105 = 3 \cdot 5 \cdot 7$ may be useful in the following questions. Be sure to verify (briefly) that your examples are in fact examples of what is requested.

(a) Give an example of nonzero congruence classes $[a]_{105}$ and $[b]_{105}$ such that $[a]_{105}[b]_{105} = [0]_{105}$.

▶ **Solution.** $[15]_{105} \cdot [7]_{105} = [105]_{105} = [0]_{105}$ but $[15]_{105} \neq [0]_{105}$ and $[7]_{105} \neq [0]_{105}$. ◀

(b) Solve the equation $[2]_{105}[x]_{105} = [1]_{105}$.

▶ **Solution.** $2 \cdot 53 = 106 = 1 + 105$ so $2 \cdot 52 \equiv 1 \pmod{105}$. Hence $[x]_{105} = [53]_{105}$. ◀

(c) Show that the congruence $6x \equiv 31 \pmod{105}$ has no solutions.

▶ **Solution.** $d = (6,\ 105) = 3$ and $3 \nmid 31$ so by Theorem 1.3.5, Page 28, there are not solutions to the congruence. ◀

6. [16 Points] Let $\sigma \in S_6$ be the permutation given in two-rowed notation by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 3 & 5 & 1 \end{pmatrix}.$$

(a) Write σ in disjoint cycle form. Is σ a cycle?

▶ **Solution.** $\sigma = (1,\ 4,\ 3,\ 6)$ is a 4-cycle. ◀

(b) Write σ^2 and σ^{-1} in disjoint cycle form.

▶ **Solution.** $\sigma^2 = (1,\ 3)(4,\ 6)$ and $\sigma^{-1} = (1,\ 6, m\,3,\ 4)$. ◀

(c) Write down a 2-cycle that commutes with σ.

▶ **Solution.** $(2, 5)$ commutes with σ since they are disjoint cycles (Theorem 2.3.4 Page 77). ◀

(d) Write down a 2-cycle that does not commute with σ.

▶ **Solution.** Any 2-cycle except for (2, 5) will work, but whichever is chosen requires verification. For example, let $\tau = (1,\ 2)$. Then $\sigma\tau = (1,\ 4,\ 3,\ 6)(1,\ 2) = (1,\ 2,\ 4,\ 3,\ 6)$ while $\tau\sigma = (1,\ 2)(1,\ 4,\ 3,\ 6) = (1,\ 4,\ 3,\ 6,\ 2)$, so that $\sigma\tau \neq \tau\sigma$. ◀