

**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]

- Find the quotient  $q$  and remainder  $r$  when 525 is divided by 231.
- Calculate the greatest common divisor  $d = (525, 231)$  by the Euclidean algorithm.
- Using Part (a), write  $d$  in the form  $s \cdot 525 + t \cdot 231$  for some integers  $s$  and  $t$ .

2. [14 Points]

- Find all solutions to the congruence  $32x \equiv 7 \pmod{101}$ . The identity

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

which may be useful, can be assumed.

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

3. [20 Points]

- If  $a$  and  $b$  are integers, write the definition of the statement “ $a$  divides  $b$ ”. Be sure to write in a complete sentence.
- 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  $a|c$ .

4. [20 Points]

- Complete the following statement of Euclid’s Lemma: *If  $p$  is a prime and  $a$  and  $b$  are integers such that  $p|ab$ , then*
- Let  $a$  and  $b$  be integers. Prove that if  $5|ab$ , then  $25|a^2$  or  $25|b^2$ .

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.

- Give an example of nonzero congruence classes  $[a]_{105}$  and  $[b]_{105}$  such that  $[a]_{105}[b]_{105} = [0]_{105}$ .
- Solve the equation  $[2]_{105}[x]_{105} = [1]_{105}$ .
- Show that the congruence  $6x \equiv 31 \pmod{105}$  has no solutions.

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

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

- Write  $\sigma$  in disjoint cycle form. Is  $\sigma$  a cycle?
- Write  $\sigma^2$  and  $\sigma^{-1}$  in disjoint cycle form.
- Write down a 2-cycle that commutes with  $\sigma$ .
- Write down a 2-cycle that does not commute with  $\sigma$ .