Name: _____

Directions: Show all work. No credit for answers without work.

1. [**6 points**] An adversary's sensitive plaintext message is encrypted with a substitution cipher, and the resulting ciphertext has been intercepted. You are asked to break the encryption and recover the plaintext message. What is the first thing you should do? Be specific.

2. [**6 points**] Encrypt the message "spy found" using the shift cipher with key $k = 3$.

3. [**4 parts, 4 points each**] For the given pairs (a, b), find the quotient q and remainder r when a is divided by b.

   (a) $a = 0$, $b = 5$

   (b) $a = 23$, $b = 8$

   (c) $a = 35$, $b = -4$

   (d) $a = -50$, $b = 7$

4. [**6 points**] Suppose that a and b are integers, $a \mid b$, and $b \mid a$. What can we conclude about a and b?

5. [**6 points**] Let a, b, and c be positive integers. One of the following statements is true and the other is false. Identify the **false** statement and give examples of integers a,b, and c which show the statement is false.

   (a) If $ab \mid c$, then $a \mid c$ and $b \mid c$.   (b) If $a \mid bc$, then $a \mid b$ or $a \mid c$.

6. [**10 points**] Let $a = 61903$, $b = 40267$, and $d = \gcd(a, b)$. Use the extended Euclidean algorithm to find d and integers u, v such that $ua + vb = d$.

7. [**2 parts, 6 points each**] EEA analysis. Suppose $a \geq b$.

   (a) How many arithmetic operations does the extended Euclidean algorithm perform when called on inputs a and b?

   (b) In what sense does the extended Euclidean algorithm perform a linear number of arithmetic operations?

8. [**2 parts, 6 points each**] Give the following tables.

   (a) The addition table for $\mathbb{Z}_5$.   (b) The multiplication table for $\mathbb{Z}_5$.

9. [**6 points**] List all the members of the ring $\mathbb{Z}_{21}$ that **do not** have inverses.

10. [**8 points**] Suppose that $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Prove that $a + b \equiv a' + b' \pmod{m}$.

11. [**12 points**] Solve for x in $782x \equiv 32 \pmod{1125}$.