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. **[14 Points]**

   (a) Compute $d = \gcd(195, 546)$.

   (b) Find integers u and v such that

   $$d = \gcd(195, 546) = 195u + 546v.$$

2. **[20 Points]** Determine whether each of the following statements about natural numbers a, b, c is true or false. Read *carefully* and pay attention to detail. If a statement has even *one* counterexample, it is false. For this exercise, record your answer in the box at the right of the statement. Explanations are not required.

   (a) If $a|b$ and $b|c$, then $a|c$. ☐

   (b) If $a|b$ and $a|c$, then $a|bc$. ☐

   (c) If $a|bc$, then $a|b$ or $a|c$. ☐

   (d) If $7|a^2$, then $7|a$. ☐

   (e) If $6|a^2$, then $6|a$. ☐

   (f) If $12|a^2$, then $12|a$. ☐

   (g) If $a|b$ and $a|c$ then $a|(b+c)$. ☐

   (h) If $a|(b+c)$ and $a|b$, then $a|c$. ☐

   (i) If $a|(b+c)$, then either $a|b$ or $a|c$. ☐

   (j) If a is prime, then no matter what b is, either $\gcd(a, b) = 1$ or $\gcd(a, b) = a$. ☐

3. **[12 Points]** This problem concerns arithmetic modulo 20. All answers should only involve expressions of the form $[a]_{20}$ with a an integer satisfying $0 \leq a < 20$. Recall that $[a]_n$ denotes the congruence class of a modulo n, and $\mathbb{Z}_n$ is the set of all congruence classes modulo n.

   (a) Compute $[9]_{20} + [16]_{20}^2$.

   (b) Compute $[9]_{20}[16]_{20}$.

   (c) Compute $[7]_{20}^{-1}$. (Recall that $[a]_n^{-1} = [b]_n$ if and only if $[a]_n[b]_n = [1]_n$, i.e. if and only if the congruence $ax \equiv 1 \pmod{n}$ is solvable.)

   (d) List the invertible elements of $\mathbb{Z}_{20}$.

4. **[14 Points]** This exercise is concerned with the solvability of the congruence equation

$$ax \equiv c \pmod{m},$$

where a, c, and m are integers with $m \geq 1$. Let $g = \gcd(a, m)$.

(a) Fill in the blanks of the following two statements (using appropriate properties of a, c, m, and g) to complete the two parts of the Linear Congruence Theorem proved in class, and in the notes:

i. If $\boxed{}$, then the congruence $ax \equiv c \pmod{m}$ has no solutions.

ii. If $\boxed{}$, then the congruence $ax \equiv c \pmod{m}$ has exactly $\boxed{}$ incongruent solutions.

(b) For each of the following linear congruences, determine the number of incongruent solutions. You need not write down the actual solutions.

i. $35x \equiv 42 \pmod{90}$

ii. $35x \equiv 42 \pmod{91}$

5. **[16 Points]** This exercise makes use of the following equation:

$$1 = 15 \cdot 27 - 4 \cdot 101.$$

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

(a) Solve the congruence equation $15x \equiv 1 \mod 101$.

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

$$\begin{aligned} x &\equiv 7 \mod 101 \\ x &\equiv 3 \mod 27. \end{aligned}$$

How are all of the other solutions related to the one you found?

6. **[12 Points]**

(a) Compute $\varphi(100)$. As usual $\varphi(n)$ denotes the Euler φ-function applied to n.

(b) Compute $11^{243} \mod 100$.

(c) What are the last two digits in the ordinary decimal expansion of 11^{243}?

7. **[12 Points]** Give the proof, using Euclid's argument, that there are infinitely many prime integers.

Bonus [3 Points] Find an explicit counterexample to the following statement concerning integers a, b, c: *If $a|c$ and $b|c$, then* $\operatorname{lcm}(a, b) \leq c$.