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

   ▶ **Solution.** Use the Euclidean algorithm:

   $$\begin{aligned} 546 &= 2 \cdot 195 + 156 \\ 195 &= 156 + 39 \\ 156 &= 4 \cdot 39 + 0. \end{aligned}$$

   Hence $\gcd(195, 546) = 39$. ◀

   (b) Find integers u and v such that

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

   ▶ **Solution.** Reverse the calculations done in part (a):

   $$\begin{aligned} 39 &= 195 - 156 \\ &= 195 - (546 - 2 \cdot 195) \\ &= 3 \cdot 195 - 546. \end{aligned}$$

   Thus, $u = 3$, $v = -1$. ◀

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 $a|c$. **T**

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

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

   (d) If $7|a^2$, then $7|a$. **T**

   (e) If $6|a^2$, then $6|a$. **T**

   (f) If $12|a^2$, then $12|a$. **F**

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

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

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

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

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 $[9]_{20} + [16]^2_{20}$.

   ▶ **Solution.** $[9]_{20} + [16]^2_{20} = [9]_{20} + [-4]^2_{20} = [9]_{20} + [16]_{20} = [25]_{20} = [5]_{20}$. ◀

   (b) Compute $[9]_{20}[16]_{20}$. **Answer:** $[4]_{20}$.

   (c) Compute $[7]^{-1}_{20}$. (Recall that $[a]^{-1}_n = [b]_n$ 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.) **Answer:** $[3]_{20}$.

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

$$\{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20}, [17]_{20}, [19]_{20}\}.$$

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

      ii. If $\boxed{g \mid c}$, then the congruence $ax \equiv c \pmod{m}$ has exactly $\boxed{g}$ 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. $35x \equiv 42 \pmod{90}$

      ▶ **Solution.** Since $\gcd(35, 90) = 5$ and $5 \nmid 42$, there are no solutions. ◀

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

      ▶ **Solution.** Since $\gcd(35, 91) = 7$ and $7 \mid 42$, there are 7 incongruent solutions. ◀

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 $15x \equiv 1 \mod 101$.

► **Solution.** The given equation means that $15 \cdot 27 \equiv 1 \pmod{101}$. Since there is exactly one solution modulo 101, all solutions are given by

$$x = 27 + 101k, \quad k \in \mathbb{Z}.$$

◄

(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?

► **Solution.** One solution is obtained from the given equation by $x = 7 \cdot (15 \cdot 27) - 3 \cdot (4 \cdot 101) = 1623$. All other solutions x are related to this one by congruence: $x \equiv 1623 \pmod{27 \cdot 101}$, i.e., $x \equiv 1623 \pmod{2727}$. Hence, $x = 1623$ is the smallest positive solution. ◄

6. **[12 Points]**

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

► **Solution.** $\varphi(100) = \varphi(25 \cdot 4) = \varphi(25)\varphi(4) = 20 \cdot 2 = 40$. ◄

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

► **Solution.** By Euler's theorem, $a^{40} = a^{\varphi(100)} \equiv 1 \pmod{100}$ for all integers a, relatively prime to 100. Since $\gcd(11, 100) = 1$, it follows that

$$11^{243} = 11^{6 \cdot 40 + 3} = (11^{40})^6 11^3 \equiv 11^3 \equiv 1331 \equiv 31 \pmod{100}.$$

◄

(c) What are the last two digits in the ordinary decimal expansion of 11^{243}? **Answer:** 31.

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

Proof. Suppose that there are only finitely many primes, which we will label as p_1, p_2, …, p_r. We will show that this assumption leads to a contradiction. Let N be the natural number defined by $N = (p_1 p_2 \cdots p_r) + 1$. Since N is a natural number, it is divisible by some prime number q. Since all prime numbers are included in our list, we must have $q = p_j$ for some j. Then, $q|N$ and $q = p_j$ so $q|(p_1 p_2 \cdots p_r)$ so q divides $N - (p_1 p_2 \cdots p_r) = 1$. But 1 has no divisors except for ± 1 and these two numbers are not primes. Hence we have shown that q is both a prime and not a prime. This contradiction means that our original assumption that there are only finitely many primes is false. Hence we must have infinitely many primes. □

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

One Example: $a = b = 2$, $c = -2$.