E. Dummit's Math 3527 ~ Number Theory 1, Spring 2026 ~ Homework 4, due Fri Feb 6th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. Use of generative AI in any manner is not allowed on this or any other course assignments.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each integer a and modulus m, determine whether the residue class $\overline{a}$ is a unit modulo m, or a zero divisor modulo m. If $\overline{a}$ is a unit then find its multiplicative inverse, while if $\overline{a}$ is a zero divisor then find a nonzero residue class $\overline{x}$ such that $\overline{x} \cdot \overline{a} = \overline{0}$.

   (a) $a = 14$, $m = 49$.
   (b) $a = 16$, $m = 49$.
   (c) $a = 125$, $m = 2026$.
   (d) $a = 788$, $m = 2026$.

---

2. Find the general solution to each of the given congruences, or explain why there is no solution:

   (a) $4n + 3 \equiv 2 \pmod{19}$.
   (b) $3n \equiv 7 \pmod{21}$.
   (c) $3n \equiv 9 \pmod{21}$.
   (d) $15n \equiv 4 \pmod{77}$.
   (e) $26n \equiv 130 \pmod{2026}$.

---

3. Using the Chinese Remainder Theorem or otherwise, find the general solution n to each system of simultaneous congruences:

   (a) $n \equiv 4 \pmod{11}$ and $n \equiv 1 \pmod{15}$.
   (b) $n \equiv 7 \pmod{999}$ and $n \equiv 37 \pmod{1001}$.
   (c) $n \equiv 7 \pmod{84}$ and $n \equiv 21 \pmod{35}$.
   (d) $n \equiv 7 \pmod{85}$ and $n \equiv 21 \pmod{34}$.
   (e) $n \equiv 2 \pmod{8}$, $n \equiv 1 \pmod{5}$, and $n \equiv 3 \pmod{9}$.
   (f) $n \equiv 1 \pmod{44}$, $n \equiv 81 \pmod{90}$, and $n \equiv 61 \pmod{80}$.

---

4. Calculate each of the following things:

   (a) The orders of each of the units modulo 9.
   (b) The order of 2 modulo 31.
   (c) The order of 3 modulo 40.
   (d) The order of -11 modulo 17.
   (e) The orders of 2, 4, and 8 modulo 25.
   (f) The order of 3 modulo 23.
   (g) The smallest positive integer s such that $3^s \equiv 1 \pmod{11}$.
   (h) The remainder when 2^{4000} is divided by 41.
   (i) The remainder when 3^{65} is divided by 17.

Part II: Solve the following problems. Justify all answers with rigorous, clear explanations.

5. Suppose n is an integer.

   (a) Show that $n^5 - n \equiv 0 \pmod{30}$. [Hint: By the Chinese Remainder Theorem, this is equivalent to showing $n^5 - n$ is divisible by 2, 3, and 5.]

   (b) Show that $n^8 - n^2 \equiv 0 \pmod{84}$.

---

6. Let $m \geq 2$ be an integer. The goal of this problem is to study the value of $(m-1)!$ modulo m.

   (a) If m is prime, show that $(m-1)! + 1$ is divisible by m.

   (b) Show that $m = 4$ is a counterexample to the statement of the proposition below, and identify the error in the proof:
   Proposition: If m is composite, then $(m-1)!$ is divisible by m.
   Proof: Suppose $m = ab$ where a and b are greater than 1 and less than m. Then both a and b appear as terms in the product $(m-1)! = (m-1) \cdot (m-2) \cdots 2 \cdot 1$, so $(m-1)!$ is divisible by ab.

   (c) If m is composite and greater than 4, prove that $(m-1)!$ is in fact divisible by m.

---

7. Prove that 5 has order 16 modulo 102 and order 36 modulo 111.

---

8. The goal of this problem is to discuss elements of order 2 and order 4 modulo m.

   (a) If $p > 2$ is prime, show that there is a unique element of order 2 in $\mathbb{Z}/p\mathbb{Z}$. [Hint: If k has order 2, then p divides $k^2 - 1 = (k-1)(k+1)$.]

   (b) Show using an example that if m is composite, then there may be more than one element of order exactly 2 in $\mathbb{Z}/m\mathbb{Z}$.

   (c) Show that an element a has order 4 in $\mathbb{Z}/m\mathbb{Z}$ if and only if its square a^2 has order 2.

   (d) Deduce that if $p > 2$ is prime, then the elements of order 4 in $\mathbb{Z}/p\mathbb{Z}$ are the elements a with $a^2 \equiv -1 \pmod{p}$.
