MATH 310 Midterm Exam 17 October 2022 2:00–2:50 p.m.

Name: _____

Show complete work—that is, all the steps needed to completely justify your answer. Simplify your answers as much as possible. You may refer to theorems in the class notes.

1. Take a deep breath. You can do this!
   (a) Tell me your favorite prime number p.
   (b) Perform the Euclidean algorithm to compute the gcd of p and 31.
   (c) Explain where you computed the multiplicative inverse of p mod 31 along the way.

2. (a) Find all solutions to $2x \equiv 2 \pmod{16}$.
   (b) Find all solutions to $5x \equiv 2 \pmod{210}$.

   Solution:

   (b) There are $\gcd(2, 16) = 2$ solutions modulo 16. The congruence can be reduced to $x \equiv 1 \pmod 8$, so the original congruence has the solutions $x \equiv 1, 9 \pmod{16}$.
   (c) $\gcd(5, 210) = 5$ does not divide 2, so there is no solution.

3. Suppose $\gcd(a, 561) = 1$.
   (a) Prove that $a^{560} \equiv 1 \pmod m$ for $m = 3$, 11, and 17.
   (b) Deduce that $a^{560} \equiv 1 \pmod{561}$.

   Solution:

   (a) Because $561 = 3 \cdot 11 \cdot 17$, $\gcd(a, 561) = 1$ means that a is relatively prime to any of these m's. So we can use Fermat's Little Theorem:
   $$a^{560} = \left(a^2\right)^{280} \equiv 1 \pmod 3$$
   $$a^{560} = \left(a^{10}\right)^{56} \equiv 1 \pmod{11}$$
   $$a^{560} = \left(a^{16}\right)^{35} \equiv 1 \pmod{17}\ .$$
   (b) This means that 3, 11, and 17 divide $a^{560} - 1$, and hence (because 3, 11, and 17 are pairwise relatively prime) so does $561 = 3 \cdot 11 \cdot 17$. (One could also invoke the Chinese Remainder Theorem here.)

   (You might have read somewhere that a composite number m is called a *Carmichael number* if the congruence $a^{m-1} \equiv 1 \pmod m$ is true for all a that are relatively prime to m. We just proved that 561 is a Carmichael number.)

4. Let p be a prime number and k a positive integer. Explain why $\sigma(p^k) = \dfrac{p^{k+1} - 1}{p - 1}$.

   Solution: The divisors of p^k are $1, p, p^2, \ldots, p^k$, and so (using a finite geometric series)
   $$\sigma(p^k) \ = \ 1 + p + p^2 + \cdots + p^k \ = \ \frac{p^{k+1} - 1}{p - 1}\,.$$