The purpose of these problems is to demonstrate that you understand the number-theoretic algorithms presented in class. You may use a computer for these problems, but you may only use the basic arithmetic operations of addition, subtraction, multiplication, division, and reduction modulo \( n \). Show enough steps that I can see that you know how the procedures work.

Do any 6 problems.

1. (a) Use the Euclidean algorithm to find the greatest common divisor of \( 262458 \) and \( 18564 \).

   (b) Find a positive integer \( x \) such that \( 6851x \equiv 1 \pmod{110934} \).

2. Compute \( 58^{36} \pmod{402} \). [No built-in exponentiation allowed.]

3. Compute \( \phi(10!) \).

4. Solve the system of equivalences

   \[
   x \equiv 68 \pmod{73} \\
   x \equiv 24 \pmod{71} \\
   x \equiv 19 \pmod{60}
   \]

5. (a) List the elements of the cyclic subgroup \( \langle 7 \rangle \) of \( \mathbb{Z}_{43}^* \).

   (b) Use part (a) to compute \( 7^{2500} \pmod{43} \).

6. Let \( a, b \) and \( c \) be positive integers.

   (a) Show that \( 2^a \equiv 2^{a\pmod{c}} \pmod{2^c - 1} \). [Hint: if \( a = qc + r \) then \( 2^a = (2^c)^q \cdot 2^r \).]

   (b) Show that \( \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1 \). [Hint: use Euclid’s lemma and part (a).]

   (c) Find 4 pairwise relatively prime numbers, each of which has at least 60 binary digits. (You do not have to represent the numbers using binary digits or decimal digits.)

   (Remark: if you can’t do one of the parts of this problem, you may still use the result of that part to do the next part.)

7. Let \( n \) be a positive integer. Prove the assertion made in class that if \( a, b \in \mathbb{Z}_n^* \), then \( ab \in \mathbb{Z}_n^* \). In other words, if \( \gcd(a, n) = \gcd(b, n) = 1 \) then \( \gcd(ab, n) = 1 \). [Hint: slide 4.3.]