Assignment 3 (submit by March 18, 2021)

Instruction: Notations used are as explained in the class.

1. For each integer below, use **extended Euclidean algorithm** to find the inverse in Z_{2555}, if the inverse exists: (a) 98, (b) 1972.

2. Let a and b be positive integers and let $n \geq ab - a - b + 1$. Show that every n-th power of an integer can be written as the product of an a-th power and b-th power.

3. Suppose you have only 13-dollar and 7-dollar bills. You need to pay someone 71 dollars. Is this possible without receiving change? If so, show how to do it. If not, explain why it is impossible.

4. Find all solutions for each of the following congruences: (a) $25x \equiv 55 \pmod{95}$, (b) $1972x \equiv 363 \pmod{2555}$.

5. Apply the Chinese Remainder Theorem to solve the following system of congruences:

$$\begin{aligned} x &\equiv 12 \pmod{25} \\ x &\equiv \ \ 9 \pmod{26} \\ x &\equiv 23 \pmod{27} \end{aligned}$$

6. Perform the modular exponentiation $22^{1437} \pmod{53}$ using
   (a) **Fast Modular Exponentiation**, (b) **Fermat's little theorem**.
   (Write your answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.)

7. Use **Euler's theorem** to compute the modular exponentiation $13^{32149} \pmod{15}$.
   (Write your answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.)

8. Compute each of the following orders, if they exist: (a) $\mathsf{ord}_{11}(5)$, (b) $\mathsf{ord}_{17}(2)$, (c) $\mathsf{ord}_{427}(21)$.

9. For $n = 81$, do the following:
   - (a) Determine whether there are any primitive roots mod $n = 81$; if so, how many will there be?
   - (b) If there are primitive roots mod $n = 81$, find the smallest one.
   - (c) If there are primitive roots, use the one you found in (b) to construct another.

10. (a) Verify that $g = 3$ is a primitive root of 566.
   - (b) How many integers mod 566 have order 12? If such elements exist, find one. (Use **order of powers formula**.)
   - (c) How many integers mod 283 have order 94? If such elements exist, find one.

——-The End———