ENEE/CMSC/MATH 456: Cryptography
Chinese Remainder Theorem Class Exercise 4/13/22

1. Use the method described in class to find the unique number x modulo 35 such that:

$$x \bmod 7 = 4$$
$$x \bmod 5 = 2$$

We first look for the elements x_1, x_2 modulo 35 that map to the basis elements (1, 0) and (0,1).
Thus x_1 is such that x_1 mod 7 = 1 and x_1 mod 5 = 0.
x_2 is such that x_2 mod 7 = 0 and x_2 mod 5 = 1.
To find x_1, x_2, we find X, Y such that 7X + 5Y = 1. Then x_1 = 5Y and x_2 = 7X.
Note that 7*(-2) + 5(3) = 1.
So x_1 = 15 and x_2 = -14.
Thus (4,2) = 4*(1,0) + 2*(0,1) -> 4*x_1 + 2*x_2 = 4*15+2(-14) = 60-28= 32.
Final answer: x = 32.

2. Use the method described in class to find the unique number x modulo 56 such that:

$$x \bmod 7 = 5$$
$$x \bmod 8 = 3$$

We first look for the elements x_1, x_2 modulo 56 that map to the basis elements (1, 0) and (0,1).
Thus x_1 is such that x_1 mod 7 = 1 and x_1 mod 8 = 0.
x_2 is such that x_2 mod 7 = 0 and x_2 mod 8 = 1.
To find x_1, x_2, we find X, Y such that 7X + 8Y = 1. Then x_1 = 8Y and x_2 = 7X.
Note that 7*(-1) + 8(1) = 1.
So x_1 = 8 and x_2 = -7.
Thus (5,3) = 5*(1,0) + 3*(0,1) -> 5*x_1 + 3*x_2 = 5*8+3(-7) = 40-21= 19.
Final answer: x = 19.