1.(1 pt) The goal of this exercise is to practice finding the inverse modulo m of some (relatively prime) integer n. We will find the inverse of 16 modulo 67, i.e., an integer c such that $16c \equiv 1 \pmod{67}$.)
First we perform the Euclidean algorithm on 16 and 67:
67 = 4* _____ + _____
_____ = _____ *5 +1
[Note your answers on the second row should match the ones on the first row.]

Thus gcd(16,67)=1, i.e., 16 and 67 are relatively prime.
Now we run the Euclidean algorithm backwards to write $1 = 67s + 16t$ for suitable integers s, t.
$s =$ _____
$t =$ _____

when we look at the equation $67s + 16t \equiv 1 \pmod{67}$, the multiple of 67 becomes zero and so we get
$16t \equiv 1 \pmod{67}$. Hence the multiplicative inverse of 16 modulo 67 is _____

2.(1 pt) Find the smallest positive integer x that solves the congruence:
$10x \equiv 5$ modulo 63
$x =$ _____

(Hint: From running the Euclidean algorithm forwards and backwards we get $1 = s(10) + t(63)$. Find s and use it to solve the congruence.)

3.(1 pt) We will find the smallest positive integer x that solves the following system of congruences via the Chinese Remainder Theorem:
$x \equiv 1 \bmod 3$
$x \equiv 5 \bmod 11$
$x \equiv 12 \bmod 17$
$x \equiv 12 \bmod 47$

In the language of Theorem 4 from page 142 of the 4th edition of Rosen, we thus have the values of the following variables:
$a_1 = 1$ and $m_1 = 3$
$a_2 = 5$ and $m_2 = 11$
$a_3 = 12$ and $m_3 = 17$
$a_4 = 12$ and $m_4 = 47$

The first step is to calculate $m = m_1 m_2 m_3 m_4$. When we do this we get:
$m =$ _____

The second step is to calculate the $\hat{m}_k$ which are given by the formula $\hat{m}_k = \frac{m}{m_k}$. Enter their values below:
$\hat{m}_1 =$ _____
$\hat{m}_2 =$ _____
$\hat{m}_3 =$ _____
$\hat{m}_4 =$ _____

Next we find the $\hat{y}_k$ which are given by solving

$$\hat{y}_k \hat{m}_k \equiv 1 \bmod m_k$$

Thus for example, to find $\hat{y}_1$ we need to solve

$$8789\hat{y}_1 \equiv 1 \bmod 3$$

Since we know $8789 \equiv 2 \bmod 3$, this simplifies to

$$2\hat{y}_1 \equiv 1 \bmod 3$$

Solve this either by trial and error or by using the Euclidean algorithm and enter the value of $\hat{y}_1$ below: (Use the canonical representative modulo 3.)
$\hat{y}_1 =$ _____

Similarly, to find $\hat{y}_2$ we need to solve

$$2397\hat{y}_2 \equiv 1 \bmod 11$$

Since we know $2397 \equiv 10 \bmod 11$,this simplifies to

$$10\hat{y}_2 \equiv 1 \bmod 11$$

Solve this either by trial and error or by using the Euclidean algorithm and enter the value of $\hat{y}_2$ below: (Use the canonical representative modulo 11.)
$\hat{y}_2 =$ _____

Similarly, to find $\hat{y}_3$ we need to solve

$$1551\hat{y}_3 \equiv 1 \bmod 17$$

Since we know $1551 \equiv 4 \bmod 17$,this simplifies to

$$4\hat{y}_3 \equiv 1 \bmod 17$$

Solve this either by trial and error or by using the Euclidean algorithm and enter the value of $\hat{y}_3$ below: (Use the canonical representative modulo 17.)
$\hat{y}_3 =$ _____

Similarly, to find $\hat{y}_4$ we need to solve

$$561\hat{y}_4 \equiv 1 \bmod 47$$

Since we know $561 \equiv 44 \bmod 47$,this simplifies to

$$44\hat{y}_4 \equiv 1 \bmod 47$$

Solve this either by trial and error or by using the Euclidean algorithm and enter the value of $\hat{y}_4$ below: (Use the canonical representative modulo 47.)
$\hat{y}_4 =$ _____

Now that we have all the $a_k, \hat{m}_k$ and $\hat{y}_k$, use the formula $x = \sum_{k=1}^{4} a_k \hat{m}_k \hat{y}_k$ to find an integer solution x to the original system. The Chinese remainder theorem says that this x and any integer congruent modulo m to it, will solve the original system. Enter the SMALLEST positive integer solution to the original system here: _____ .

4.(1 pt) Find the SMALLEST positive integer solution to the following system of congruences:
$x \equiv 2 \bmod 5$
$x \equiv 1 \bmod 7$
The solution is _____ .

5.(1 pt) Use Fermat's Little theorem to compute the following remainders for 3^{1921} (Always use canonical representatives.)
$3^{1921} =$ _____ mod 5
$3^{1921} =$ _____ mod 7
$3^{1921} =$ _____ mod 11

Use your answers above to find the canonical representative of 3^{1921} mod 385 by using the Chinese Remainder Theorem. [Note $385 = 5 \cdot 7 \cdot 11$ and that Fermat's Little Theorem cannot be used to directly find 3^{1921} mod 385 as 385 is not a prime and also since it is larger than the exponent.]

3^{1921} mod 385 is _____

6.(1 pt) Fill in the blanks in the table with the unique integers a in the range $0 \leq a \leq 27$ with the given remainders.

Hint: It is probably easiest to just make a table with the numbers between 0 and 27 and their remainders and use that to find the answers. However one can also use the Chinese Remainder Formula

$x = a_1\hat{m}_1\hat{y}_1 + a_2\hat{m}_2\hat{y}_2$ by finding the $\hat{m}_k, \hat{y}_k$ once and then plugging in the various remainders for the a_k to get the various answers.

a	a mod 4	a mod 7
__	1	3
__	0	2
__	1	1
__	3	2
__	2	5
__	0	2
__	3	6
__	2	0
__	2	3

7.(1 pt) (Modification of exercise 36 in section 2.5 of Rosen.) The goal of this exercise is to work thru the RSA system in a simple case:

We will use primes $p = 41, q = 61$ and form $n = 41 \cdot 61 = 2501$. [This is typical of the RSA system which chooses two large primes at random generally, and multiplies them to find n. The public will know n but p and q will be kept private.]

Now we choose our public key $e = 13$. This will work since $gcd(13, (p-1)(q-1)) = gcd(13, 2400) = 1$. [In general as long as we choose an 'e' with gcd(e,(p-1)(q-1))=1, the system will work.]

Next we encode letters of the alphabet numerically say via the usual:

(A=0,B=1,C=2,D=3,E=4,F=5,G=6,H=7,I=8,
J=9,K=10,L=11,M=12,N=13,O=14,P=15,Q=16,R=17,
S=18,T=19,U=20,V=21,W=22,X=23,Y=24,Z=25.)

We will practice the RSA encryption on the single integer 15. (which is the numerical representation for the letter "P"). In the language of the book, M=15 is our original message.

The coded integer is formed via $c = M^e$ mod n.

Thus we need to calculate 15^{13} mod 2501.

This is not as easy as it seems and you might consider using fast modular multiplication

The canonical representative of 15^{13} mod 2501 is _____