1. **(5 points)** `Library/UMass-Amherst/Abstract-Algebra/PS-Functions/Functions1.pg`
Consider the function

$$\varphi : \{3,4,...,11,12\} \to \{3,4,...,11,12\}$$

x	3	4	5	6	7	8	9	10	11	12
$\varphi(x)$	10	9	6	4	5	8	12	7	3	11

(a) Is this one-to-one? _____ (Y/N)

(b) Is this onto? _____ (Y/N)

(c) Is this bijective? _____ (Y/N)

2. **(5 points)** `Library/UMass-Amherst/Abstract-Algebra/PS-Functions/Functions2.pg`
Complete the following table of values of a function

$$\varphi : \{5,6,...,13,14\} \to \{3,4,...,11,12\}$$

x	5	6	7	8	9	10	11	12	13	14
$\varphi(x)$	7	___	___	3	6	11	___	___	8	___

so that φ is onto.

3. **(5 points)** `Library/UMass-Amherst/Abstract-Algebra/PS-Relations/Relations7.pg`

Let X be the set $\{18,10,13\}$. For the first three parts of this problem you are asked to define a function $f : X \to X$ so that the relation

$$u \sim w \Leftrightarrow w = f(u)$$

satisfies each of the following conditions.

(a) $\sim$ is reflexive

x	18	10	13
$f(x)$	___	___	___

(b) $\sim$ is symmetric

x	18	10	13
$f(x)$	___	___	___

(c) $\sim$ is transitive

x	18	10	13
$f(x)$	___	___	___

(d) [optional: see your instructor] Let Y be an arbitrary non-empty set. Determine all functions $g : Y \to Y$ so that the relation

$$a \sim b \Leftrightarrow b = g(a)$$

is
- Reflexive
- Symmetric
- Transitive

4. **(5 points)** `Library/Rochester/setDiscrete6Integers/ur_dis_6_7.pg`
Encrypt the message " HALT " by translating the letters into numbers
(via $A=0,B=1,C=2,D=3,E=4,F=5,G=6,H=7,I=8,$
$J=9,K=10,L=11,M=12,N=13,O=14,P=15,Q=16,R=17,$
$S=18,T=19,U=20,V=21,W=22,X=23,Y=24,Z=25$
)
and then applying the encryption function given, and then translating the numbers back into letters.

(a) $f(p)=(p+3)$ mod 26 ______
(b) $f(p)=(p+15)$ mod 26 ______
(c) $f(p)=(p+5)$ mod 26 ______

---

5. **(5 points)** `Library/Rochester/setDiscrete6Integers/ur_dis_6_8.pg`

Decrypt the following messages encrypted using the Caesar cipher:
$f(p)=(p+3)$ mod 26
Alphabet: A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
(a) FUDCB KDWV ______
(b) EOXH MHDQV ______
(c) HFWNESVJ ______

---

6. **(5 points)** `Library/ASU-topics/crypto/enc_aff.pg`
Encrypt the message " MATH " by translating the letters into numbers
and then applying the encryption function given, and then translating the numbers back into letters.

(a) $f(p)=(17p+4)$ mod 26 ______
(b) $f(p)=(19p+7)$ mod 26 ______
(c) $f(p)=(3p+3)$ mod 26 ______

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

---

7. **(5 points)** `Library/ASU-topics/crypto/dec_aff.pg`

Decrypt the message *YPSDPS* which was encrypted using the affine cipher:

$$f(p)=(7p+15) \bmod 26$$

Alphabet: $A=0,B=1,\ldots,Z=25$

Message: ______

---

8. **(10 points)** `Library/Rochester/setDiscrete7NumberTheory/ur_dis_7_1.pg`
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 7 modulo 45, i.e., an integer c such that $7c \equiv 1 \pmod{45}$.

First we perform the Euclidean algorithm on 7 and 45:
$45 = 6*$ ______ + ______
______ = ______ $*2 + 1$
[Note your answers on the second row should match the ones on the first row.]

Thus gcd(7,45)=1, i.e., 7 and 45 are relatively prime.

Now we run the Euclidean algorithm backwards to write $1=45s+7t$ for suitable integers s,t.
$s=$ ______
$t=$ ______
when we look at the equation $45s+7t \equiv 1 \pmod{45}$, the multiple of 45 becomes zero and so we get
$7t \equiv 1 \pmod{45}$. Hence the multiplicative inverse of 7 modulo 45 is ______

---

9. **(5 points)** `Library/Rochester/setDiscrete7NumberTheory/ur_dis_7_2.pg`

Find the smallest positive integer x that solves the congruence:

$$10x \equiv 2 \pmod{63}$$

$x=$ ____

(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.)

---

10. **(5 points)** `Library/Rochester/setDiscrete6Integers/ur_dis_6_3.pg`
The value of the Euler ϕ function (ϕ is the Greek letter phi) at the positive integer n is defined to be the number of positive integers less than or equal to n that are relatively prime to n. For example fon n=14, we have $\{1,3,5,9,11,13\}$ are the positive integers less than or equal to 14 which are relatively prime to 14. Thus $\phi(14)=6$. Find:
$\phi(3)$ ____
$\phi(9)$ ____
$\phi(6)$ ____
$\phi(12)$ ____

---

11. **(5 points)** `Library/Rochester/setDiscrete7NumberTheory/ur_dis_7_7.pg`
(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 $p = 71, q = 53$ and form $n = 71 \cdot 53 = 3763$. [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 $gcd(13, (p-1)(q-1)) = gcd(13, 3640) = 1$. [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 $c = M^e \bmod n$.

Thus we need to calculate $15^{13} \bmod 3763$.

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

The canonical representative of $15^{13} \bmod 3763$ is ______

---

12. **(5 points)** `Library/Rochester/setDiscrete7NumberTheory/ur_dis_7_4.pg`
Find the SMALLEST positive integer solution to the following system of congruences:

$$x \equiv 0 \pmod 3$$
$$x \equiv 6 \pmod 7$$

The solution is ______.

---

13. **(5 points)** `Library/SDSU/Discrete/IntegersAndRationals/pL11.pg`

Find the smallest positive integer x such that:
$x \bmod 2 = 1$
$x \bmod 3 = 2$ and
$x \bmod 5 = 3$
___

What is the next integer with this property?
___

[You will have to do some trial and error, but thinking about divisiblity should lead you to some patterns.]