1. **(4 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:
$\phi(2)$ ____
$\phi(4)$ ____
$\phi(10)$ ____
$\phi(50)$ ____

2. **(6 points)** `Library/SDSU/Discrete/IntegersAndRationals/pL7.pg`

Find the smallest positive integer for which
$x \bmod 3 = 2$ and $x \bmod 4 = 3$
___

What is the next smallest integer with this property?

___

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

3. **(6 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.]

4. **(6 points)** `Library/UMass-Amherst/Abstract-Algebra/PS-Congruences/Congruences5.pg`

Solve each of the following congruences. Make sure that the number you enter is in the range $[0, M-1]$ where M is the modulus of the congruence. If there is more than one solution, enter the answer as a list separated by commas. If there is no answer, enter N.

(a) $151x = 1 \pmod{374}$

$x =$ ____

(b) $114x = 116 \pmod{374}$

$x =$ ____

5. **(8 points)** `Library/Rochester/setDiscrete7NumberTheory/ur_dis_7_5.pg`
Use Fermat's Little theorem to compute the following remainders for 3^{963} (Always use canonical representatives.)
$3^{963} =$ ____ mod 5
$3^{963} =$ ____ mod 7
$3^{963} =$ ____ mod 11

Use your answers above to find the canonical representative of 3^{963} 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^{963} mod 385 as 385 is not a prime and also since it is larger than the exponent.]
3^{963} mod 385 is ________

6. **(6 points)** `Library/UMass-Amherst/Abstract-Algebra/PS-Congruences/Congruences1.pg`
Perform the following congruence computations. Make sure that the number you enter is ≥ 0 and $\leq N-1$, where N is the modulus of the congruence.

$7685 + 6984 \equiv$ ____ $\pmod{52}$
$5994 - 52 * 9344 \equiv$ ____ $\pmod{47}$
$10775+$ ____ $-264 \equiv 764 * 646 \pmod{41}$
$497 * (54323 - 692) * 4494 - 556 \equiv$ ____ $\pmod{40}$
$3920^2 \equiv$ ____ $\pmod{87}$)

7. **(6 points)** `Library/UMass-Amherst/Abstract-Algebra/PS-Congruences/Congruences6.pg`

Which of the following values are needed to compute 3^{104} (mod 41) using fast exponentiation? Mark Y/N accordingly:

i	3^{2^i} (mod 41)	Y/N
0	3	____
1	9	____
2	40	____
3	1	____
4	1	____
5	1	____
6	1	____
7	1	____

Use these values to compute 3^{104} (mod 41)

3^{104} (mod 41) = ____

---

8. **(6 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) $f(p)=(p+4)$ mod 26 ________
(b) $f(p)=(p+13)$ mod 26 ________
(c) $f(p)=(p+3)$ mod 26 ________

---

9. **(6 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) HDW GLP VXP ________
(c) FEPGYTRD ________

---

10. **(6 points)** `Library/ASU-topics/crypto/dec_aff.pg`

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

$$f(p)=(21p+20) \bmod 26$$

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

Message: ________

---

11. **(6 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) $f(p)=(19p+4)$ mod 26 ________
(b) $f(p)=(3p+11)$ mod 26 ________
(c) $f(p)=(11p+5)$ mod 26 ________

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

---

12. **(8 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 $p=43, q=47$ and form $n=43\cdot 47=2021$. [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 $e=17$. This will work since $gcd(17,(p-1)(q-1))=gcd(17,1932)=1$. [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^{17} mod 2021.

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

The canonical representative of 15^{17} mod 2021 is ________