

Names : \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_ .

### Project #3 Elementary Number Theory

The expression  $\mathbf{gcd}(m,n)$  stands for the greatest integer that divides both the integers  $m$  and  $n$ . The expression  $\mathbf{lcm}(m,n)$  stands for the least integer which is a multiple of both the integers  $m$  and  $n$ .

Following the procedures of the first project, compute each of the following integers.

	HAND	CAL	CAS	Comments
gcd(6,8)				
lcm(6,8)				
product of two previous numbers				
product of 6 & 8				
gcd(48,80)				
lcm(48,80)				
product of two previous numbers				
product of 48 & 80				
gcd(140,429)				
lcm(140,429)				
product of two previous numbers				
product of 140 & 429				

*Exercise.* Experiment with several different pairs of integers  $m$  and  $n$  computing  $\mathbf{gcd}(m,n) \cdot \mathbf{lcm}(m,n)$  and  $m \cdot n$ . What relationship is suggested by your experiment?

Continuing with examples, but just using computational devices to facilitate the actual calculations:

	CAL	CAS	Comments
$\gcd(101+45, 36^2)$			
$\text{lcm}(5(1+4^3), 2^5)$			
$\frac{36}{\gcd(36,16)}$			
$\frac{\text{lcm}(38,100)}{\gcd(38,100)}$			
$\text{lcm}(1524, 5567)$			
$\text{lcm}(2000, 6000)$			

Notice that the last two results show that bigger integers don't necessarily yield bigger lcm's.

	CAL	CAS	Comments
$\gcd(10^{13}, 1050)$			
$\text{lcm}(14^6, 15^{15})$			
your R#			
your friend's R#			
$\gcd(\text{your R\#, your friend's R\#})$			
$\text{lcm}(\text{your R\#, your friend's R\#})$			

### Fundamental Theorem of Arithmetic.

Two integers are said to be relatively prime if the biggest integer that divides both of them is 1.

*Exercise.* List all pairs of integers from 100 to 105 that are relatively prime.

\* You might find the programs and the end of this project to be interesting.

An integer greater than 1 is said to be prime if its only divisors are 1 and itself, otherwise it is called composite. For example 2,3,5,&7 are the only primes less than 10. What are the primes between 10 and 50?

The Maple command "isprime" determines whether or not a given integer is prime. You can ask a questions in WolframAlpha "Is  $n$  prime?" Use a CAS to see if the following numbers are prime. In each case leave the P if prime and leave the C if composite.

129	235	1537	your R#	$10!+1$	329891
P C	P C	P C	P C	P C	P C

The *Fundamental Theorem Of Arithmetic* states that every integer can be factored in a unique (up to order) way into a product of powers of primes.

*Exercise.* Use paper and pencil, aided by your CAL if necessary, to write each of the following numbers as a product of powers of primes:

i.  $10! =$

ii.  $340704 =$

CAS programs typically have commands to automatically factor integers into their prime power decompositions: Maple **ifactor**"; WolframAlpha **factor**. Use a CAS to compute the prime power factorization for each of the following:

i.  $10!$

ii.  $340704$

iii.  $10!+1 =$

iv.  $100! =$

iv. your R# =

(Notice how just adding 1 to  $10!$  reduced the number of prime factors.)

For two integers  $m$  and  $n$ ,  $m > 0$ , we say the remainder of  $n$  divided by  $m$  is  $r$  if  $n = qm + r$ , for integers  $q$  and  $r$  with  $0 \leq r < m$ . The Division Algorithm guarantees that the remainder  $r$  is unique.

In Maple/WolframAlphah this remainder is denoted by " $n \bmod m$ ". Your CAL may denote it as "mod(n,m)".

*Exercise* Use HAND, CAL, and CAS to compute the following remainders:

	HAND	CAL	CAS
24 mod 5			
156 mod 7			
32 mod 2			
57 mod 2			

Compute each of the following remainders using your CAL first and the CAS next.

	CAL	CAS
13200 mod 134		
$(12^3+53) \bmod 26$		
$(400*23) \bmod 18$		
$1321 \bmod (5*7)$		
$45^{16} \bmod 2$		

1

*Exercise.* In the last problem, which answer do you think is correct?

Explain

*Exercise.* Explain why an integer  $n$  is even exactly when  $n \bmod 2 = 0$ , and  $n$  is odd exactly when  $n \bmod 2 = 1$ .

Recall the statement of the **BINOMIAL THEOREM**.

$(m + n)^k =$

*Exercise.* Use the binomial theorem to explicitly expand, (ie. compute the binomial coefficients)

i.  $(x + y)^3 =$

and

ii.  $(n + 1)^4 =$

*Exercise.* Explain why every power of an odd integer must be an odd integer also.

First using the Fundamental Theorem of Arithmetic.

Second using the Binomial Theorem.

You should be able to compute each of the following **by hand**. Do so and then check your answer using both technologies. Record your results in the appropriate places.

	HAND	CAL	CAS	Comments
$1342 \bmod 2$				
$(10!+1) \bmod 2$				
$17^9 \bmod 2$				
$17^{11} \bmod 2$				
$17^{12} \bmod 2$				

*Exercise.* Explain why your CAL thinks  $17^{12}$  is even, when we, and Maple, know better.

### Modular Arithmetic.

For a fixed integer  $n$  the computation of remainders mod  $n$  obeys familiar laws of arithmetic. This arithmetic has very useful and pragmatic consequences for both theory and practice. Consider the following examples where the fixed integer is 7 and  $[x]$  denotes the congruence class of  $x \pmod{7}$

A.  $[37] = \underline{\hspace{2cm}}$

B.  $[55] = \underline{\hspace{2cm}}$

C.  $[37 * 55] = \underline{\hspace{2cm}}$

D.  $[37] * [55] = \underline{\hspace{2cm}}$

E.  $[37 + 55] = \underline{\hspace{2cm}}$

F.  $[37] + [55] = \underline{\hspace{2cm}}$

What do parts C,D and parts E,F suggest to you?

**Divisibility Rules** Determine whether the integers in the left column are divisible by the factors in the top row

	2	3	4	5	6	7	8	9	10	11	12	15	18	20	24	25	36	48	60	75
182																				
280																				
1404																				
1920																				
2320																				
2904																				
2953																				
3080																				
4572																				
4575																				
4920																				
5190																				
5400																				
5742																				
6210																				
6516																				
6552																				
7368																				
7375																				
7596																				
8586																				
8814																				
9350																				
9500																				
9918																				

**Alternate Bases** Convert the given integers from base 10 to the specified base. (For base 12 use the symbol *t* for ten and *e* for eleven:

Integer (Base 10)	New Base	Integer (New Base)
345	12	
345	7	
345	2	
1280	12	
1280	7	
1280	2	
4321	12	
4321	7	
4321	2	

**Alternate Bases (Continued)**

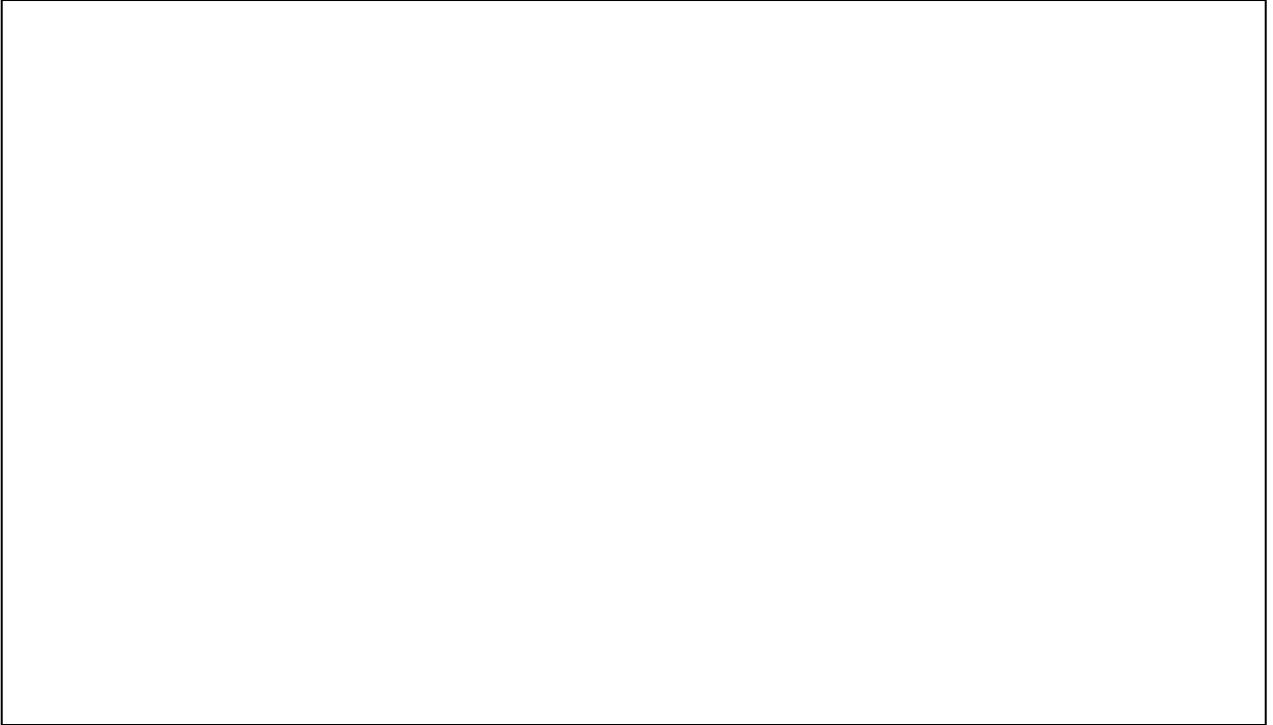
Consider the following numbers given in alternate bases in the left-hand column. Determine whether they are divisible by the (standard base 10) numbers given across the top row.

	2	3	4	5
$1010101_2$				
$1221_3$				
$314_5$				
$123_6$				
$341_7$				
$2t4_{12}$				
$306_{12}$				



*Reflection:*

1. What are the main things you learned from Chapter 3?



2. What is the hardest thing to understand from Chapter 3?



Look at the following Maple programs. Try to determine what they should do and then execute them to see if you were correct. (To move from a line of Maple input to another line without Maple wanting to execute something, hold down the shift key as you press the enter key.)

Program I

```
> for i from 1 to 100
do
  if
    isprime(i)=true
    then print(i)
  fi;
od;
```

Program II

```
> for i from 100 to 105
do
  for j from i to 105
do
  if
    gcd(i,j)=1
    then print(i,j);
  fi;
od;
od;
```