Cryptology 1 Lab—Modular Arithmetic--KEY

1. 6395 divided by 271  
   A screen shot of a computer

   Description automatically generated  
   quotient: 23 remainder: 162
2. GCD of 6395 and 271 Do the numbers share a common factor (divisor)?  
   A black screen with white text

   Description automatically generated  
   No, relatively prime.
3. 5186019 divided by 7593  
   A black background with a purple border

   Description automatically generated with medium confidence  
   quotient: 683 remainder: 0  
   Note that 7593 divides 5186019 evenly—no remainder
4. GCD of 53068020 and 7593. Do the numbers share a common factor (divisor)?  
   No, GCD not = 1

# Modular Arithmetic

Compute the following:

1. 519 + 434 + 540 (mod 601)  
   
2. 217 \* 121 \* 550 (mod 601)  
   A black background with white text

   Description automatically generated
3. 221 \* 491 + 590 (mod 601)  
   
4. 9-1 (mod 29)  
     
   A black screen with white text

   Description automatically generated
5. 7 / 3 (mod 17)  
     
   A screen shot of a computer

   Description automatically generated

# Exponentiation (Powers)

Compute the following:

1. 5012 (mod 601)  
     
   A black square with white dots

   Description automatically generated with medium confidence
2. 624541967341563 to the power 17165546346465 (mod 601)  
   If you don’t use the correct function (see class slides, slide 11) this will take a very long time. With the correct function it will be very fast. Encryption uses much larger numbers than this.  
   A black background with white numbers

   Description automatically generated

# Multiplication

The two multiplication tables below represent integer rings, ℤn.   
 What is n for Table A? Table B?  
Which one of them is also a prime field?

Why?

Table A Table B

A picture containing text, electronics, keyboard, lamp

Description automatically generated A picture containing text, indoor, white, lamp

Description automatically generated

Table A, n =5 (0 through 4, 5 elements)

Table B, n=6 (0 through 5, 6 elements)

Table A is a prime field, since n = 5 is a prime number.

Table B is NOT a prime field, 6 is not prime (composite). Also, look at rows 2, 3, and 4—they only contain some of the elements.