Cryptology 1 Lab—Modular Arithmetic

# Reading

Class Slides: Cryptology 0 Lab—Modular Arithmetic

You may complete this lab using pencil and paper, a calculator, a spreadsheet, or a programming language. I recommend Python but use whatever you like. If you choose to use Python, you will want to use modules to compute the GCD of two numbers, and the multiplicative inverse using modular arithmetic. These modules are available in the PyCryptodome package. Instructions for installing Python and PyCryptodome are available on Canvas.

Once PyCryptodome is installed, you can use its modules by importing them into your scripts or Python shell:  
from Crypto.Util.number import GCD  
from Crypto.Util.number import inverse

Once you have imported GCD and inverse, you get help through Python:  
help(GCD)  
help(inverse)

You can also read about the GCD and inverse functions here: <https://pycryptodome.readthedocs.io/en/latest/src/util/util.html#module-Crypto.Util.number>

# Integer Division and Remainders, GCD

Compute the quotient (integer division), remainder and GCD for the following numbers. You may want to check slide 11 in the class slides for Python operators that will help you.

1. 6395 divided by 271  
     
   quotient: remainder:
2. GCD of 6395 and 271 Do the numbers share a common factor (divisor)?
3. 5186019 divided by 7593  
     
   quotient: remainder:
4. GCD of 53068020 and 7593. Do the numbers share a common factor (divisor)?

# Modular Arithmetic

Compute the following:

1. 519 + 434 + 540 (mod 601)
2. 217 \* 121 \* 550 (mod 601)
3. 221 \* 491 + 590 (mod 601)
4. 9-1 (mod 29)
5. 7 / 3 (mod 17)

# Exponentiation (Powers)

Compute the following:

1. 5012 (mod 601)
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.

# 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