INFORME LABORATORIO 1

# LISTA DE CONTENIDOS

1.Lista de Contenidos  
2.Lista de Figuras  
3.Lista de Tablas  
4.Lista de Códigos  
5.Desarrollo   
 5.1. Multiplicación Modular  
 5.1. Inverso Modular  
 5.1. Exponenciación Modular   
6.Conclusiones  
7.Referencias

# LISTA DE FIGURAS Fig 1. Ejecución de la MULTIPLICACIÓN MODULAR (PAG. 3) FiG 2. Ejecución del INVERSO MODULAR (PAG. 4) Fig 3. Ejecución de una EXPONENCIACIÓN MODULAR (PAG. 5)

# LISTA DE TABLAS

# ----

# LISTA DE CÓDIGOS

# 

Cod 1. Función MODULO (Pag. 2)

Cod 2. Función MULTIPLICACIÓN MODULAR (Pag. 2)

Cod 3. Función DEL INVERSO MODULAR (Pag. 3)  
Cod 4. Función de CONVERTIR UN NUMERO A BINARIO (Pag. 4)  
Cod 5. Función EXPONENCIACIÓN MODULAR (Pag. 5)

DESARROLLO:

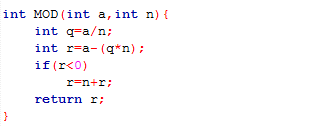
Durante las sesiones del laboratorio de práctica realizamos las operaciones básicas de la aritmética modular, teniendo presentes la multiplicación, la inversa y la exponenciación, buscando la manera de simplificarlas y que no sean de las formas convencionales.

## MULTIPLICACIÓN MODULAR

El algoritmo de multiplicación modular se usa para hallar de una manera rápida y eficaz esta operación sin tener que llegar necesariamente a números gigantescos, es por esto que utilizamos el modulo

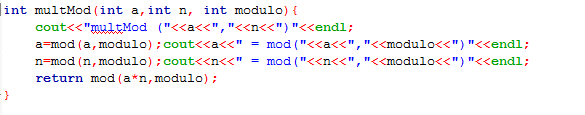
Para la implementación del algoritmo de la multiplicación modular  es necesario usar la función modulo:

**Código 1.**



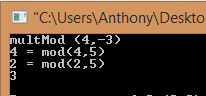
E incluí en el código del algoritmo de la multiplicación modular a continuación:

**Código 2.**



Y su ejecución en consola es la siguiente:

**Fig 1.**

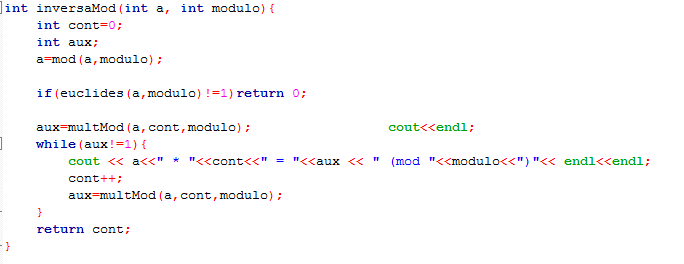


## INVERSO MODULAR

Para la implementación de la Inversa modular tome de base el algoritmo de multiplicación modular, ya que estamos en el contexto de la aritmética modular (Cod. 1).

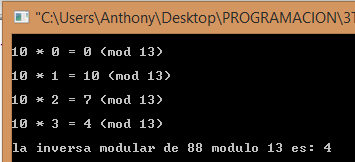
Asi, la implementación del código seria la siguiente:

**Código 3.**

****

Y la ejecución en consola, sería la siguiente:

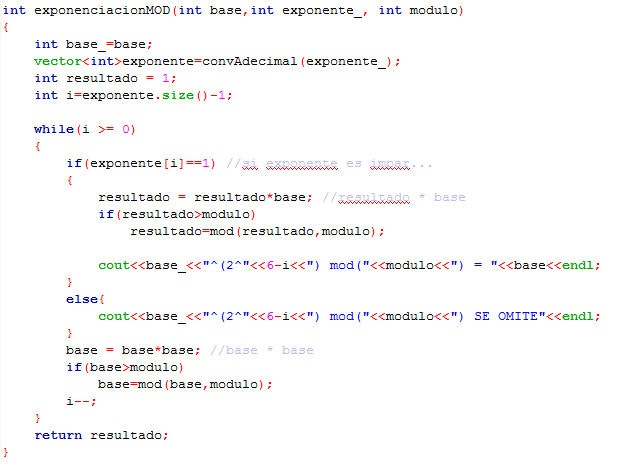
**Figura 2.**



## Exponenciación Modular

Esta implementación de la exponenciación modular usa el divisor convertido en base dos, lo que permite hacer la exponenciación mucho más rápida, solo eleva a la base cuando el bit del divisor en cierta posición está en 1.

Su implementación es la siguiente:

**Código 5.** 

Y su ejecución en consola sería la siguiente:

**Figura 3.**

# 

# CONCLUSIONES

* La multiplicación modular es básicamente lo mismo que dos números multiplicados pero con la diferencia de que esta usa clases de equivalencia, lo cual permite que la computadora no realice operaciones gigantescas que al fin y al cabo llevaran a un mismo resultado.
* La inversa modular de un número tiene su mayor potencial al usarla en la desencriptación de un mensaje cifrado por también una multiplicación modular.
* La exponenciación modular así como la multiplicación reduce significativamente el costo computacional y el tiempo ocupado al realizar demasiadas operaciones. Esta también usa clases de equivalencia.
* Esta implementación de la exponenciación modular usa el divisor convertido en base dos, lo que permite hacer la exponenciación mucho más rápida, solo eleva a la base cuando el bit del divisor en cierta posición está en 1.

# REFERENCIAS

1. Johnsonbaugh Richard (2005) Matemáticas Discretas (Sexta Edición).
2. [Grimaldi, Ralph P.](https://es.wikipedia.org/wiki/Ralph_Peter_Grimaldi) (1997). *Matemáticas Discreta y Combinatoria: Una introducción con aplicaciones* (3a edición).