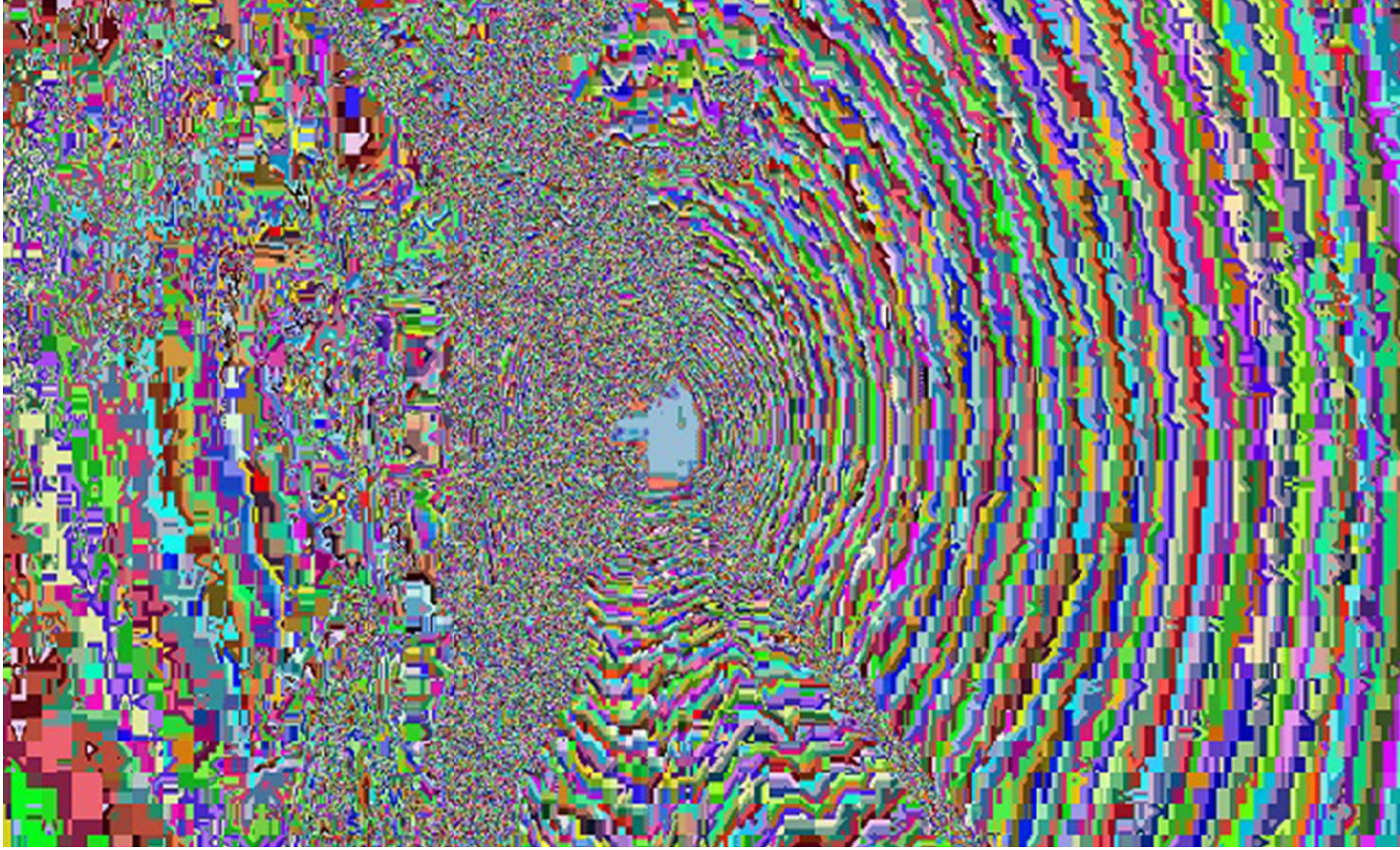


EL MÉTODO GAUSS-JACQUES PROPUESTO PARA LA OBTENCIÓN DE MATRICES INVERSAS MODULARES DE TAMAÑO VARIABLE SIN LÍMITE TEÓRICO

The proposed Gauss-Jacques method to obtain modular inverse matrices variable sized without a theoretical limit

EL MÉTODO GAUSS-JACQUES PROPUESTO PARA LA OBTENCIÓN DE MATRICES INVERSAS MODULARES DE TAMAÑO VARIABLE SIN LÍMITE TEÓRICO

M.S.I. Fausto Abraham Jacques García
Autor para correspondencia: jacques@uaq.edu.mx
Facultad de Informática, Universidad Autónoma de Querétaro.

Fecha de recepción 15/02/2018
Fecha de aceptación 22/05/2018

Resumen

El presente escrito describe la propuesta de un método desarrollado para realizar el cálculo necesario para la obtención de matrices inversas modulares de tamaño n x n con implicaciones computacionales eficientes y con aplicaciones a la criptografía simétrica. Se habla también sobre descubrimiento de fenómenos dentro de los espacios lineales aritméticos y posibles teoremas encontrados. Es un aporte importante al conocimiento y aplicación directa en problemas de seguridad de datos dentro del contexto de las ciencias computacionales. En base a las investigaciones y experimentos realizados, se observó que el método cumple con las características o atributos de ser preciso, definido y finito, por lo que se puede programar en cualquier lenguaje de computadoras. Se concluye que es un método computacionalmente eficiente y puede ser implementado en dispositivos hardware de propósito específico. Los usos y aplicaciones del método son infinitos. Lo expresado en el presente resumen, y lo encontrado en base a los experimentos, hace este escrito diferente de otros trabajos de divulgación basados en la misma área de conocimiento.

Palabras Clave: *Matrices inversas modulares, Eficiencia computacional, espacios lineales aritméticos, Criptografía simétrica.*

Abstract

This paper describes de proposal of a developed method to obtain modular inverse matrices sized n x n considering computational efficiency and applications in symmetric cryptography. It is also discussed about some phenomenon in linear arithmetic spaces and some theorems found. This work is an important contribution to knowledge and direct appliance in data security problems in computer science context. Based on research and experiments conducted, it was observed that this method is precise, defined and finite, so it can be programmed in any computer language. It is concluded that this method is computationally efficient and can be implemented in specific-driven purpose hardware. Uses and applications of this method are infinite. The expressed in this abstract, and what has been found with the experiments, make this paper different from any other divulgation works belonging to the same area of knowledge.

Key Words: *Modular inverse matrices, computational efficiency, linear arithmetic spaces, symmetric cryptography.*

1. INTRODUCCIÓN

El método Gauss-Jacques tiene registro de propiedad intelectual número: 03-2017-121413461200-01, y 1802155794464, a nivel nacional e internacional respectivamente. Cuenta también registro copyright en Estados Unidos de América (USA). Un tema que comprende de basta forma los Espacios Lineales Aritméticos, es el cálculo de las Matrices Inversas Modulares. Estas matrices tienen la propiedad de que los elementos que las componen deben pertenecer al conjunto de los números naturales, esto es, los elementos deben de ser enteros y positivos. Dentro del cálculo necesario para la obtención de una matriz inversa modular se ponen en práctica los siguientes conocimientos:

1) Método Gauss.

2) Ecuaciones lineales modulares con infinidad de soluciones.

3) Módulo Euclidiano.

4) La determinante.
5) Números primos relativos.
6) Algoritmo extendido de Euclides.
7) Ecuaciones diofánticas.
8) Congruencias.
9) Producto matricial.
10) Teoría de la combinatoria.
11) Proposiciones lógicas.
12) Relaciones matemáticas.
13) Teoría de Conjuntos.
14) El plano R2.
15) La línea recta.
16) Divisibilidad Euclidiana.

En cada uno de los momentos al proceder con el cálculo de la inversa modular de una matriz cuadrada, se usa alguno de los conceptos y operaciones listados. Al principio, se debe saber si la matriz tiene una inversa modular asociada con el módulo que se desea trabajar. Para esto se calcula la determinante de dicha matriz. Si el máximo común divisor entre el valor absoluto de la determinante de la matriz y el módulo es igual a uno, entonces significa que esa matriz si tiene una inversa modular asociada. Esto es, si el valor absoluto de la determinante de la matriz y el módulo son primos relativos. Al haber hecho esto, se procede con el proceso para obtener la forma reducida y escalonada por renglones. Para transformar el primer elemento de la matriz, se tiene que cumplir la siguiente condición:

$$a_{11}x \bmod n = 1 \quad (1)$$

Se tiene que encontrar un *x,* tal que al multiplicarse por a_{11} y aplicarse el módulo *n*, el resultado sea igual a 1. Se tiene que

$$a_{11}x = nq + 1 \quad (2)$$

Despejando *x*, se tiene que

$$x = (nq + 1)/a_{11} \quad (3)$$

Se tiene una ecuación con dos incógnitas, lo que significa que *x* puede tomar una infinidad de valores. Para encontrar el valor de *x*, y que se cumpla con la condición, se puede usar el algoritmo extendido de Euclides o simplemente realizar una tabulación hasta que *x* sea un entero. Ya que se tiene uno de los valores de x, las otras soluciones se encuentran sumando el módulo al valor encontrado. Esto es,

$$x_{n+1} = x_n + módulo \quad (4)$$

Se puede usar cualquiera de esta infinidad de soluciones, y al final, se llegará al mismo resultado. Todo el renglón correspondiente se multiplica por *x* y el resultado de esa multiplicación se opera con el módulo *n*. El resultado de lo anterior será igual a cada uno de los elementos de ese renglón. Ya que se tiene el pivote, se usa para reducir los elementos de su columna. Se reducen. Al reducirse, si se obtienen números negativos, se aplica el módulo Euclidiano. Ya que se tiene la matriz inversa modular, ésta se multiplica por la original. A la matriz resultante se le aplica el módulo *n* a cada uno de los elementos que la confirman. Si el resultado es igual a la matriz identidad, entonces se ha comprobado que la inversa modular encontrada es correcta.

A. El algoritmo de Euclides

El número entero *s* se llama divisor (o multiplicador) del número entero *n*, si *n=st* para algún t E Z. A su vez se llama múltiplo de *s*. La divisibilidad de *n* por *s* se indica con el símbolo *s*|*n*, y a la indivisibilidad con el símbolo *s*-|*n*. La divisibilidad es una relación transitiva en Z. Si, sucesivamente *m*|*n* y *n*|*m*, entonces *n=+-m*, y los números enteros *m* y *n* se llaman asociados. Según el teorema de Euclides, el conjunto *P = {2, 3, 5, 7, 11, 13, ...}* de todos los números primos es infinito (Kostrikin A.I, 1983).

Sean *m* y *n* enteros tales que no son ambos cero. Entro todos los enteros que dividen a *m* y *n*, existe un divisor más grande, conocido como el máximo

común divisor de *m* y *n*, se escribe m.c.d.(m, n) (Johnsonbaugh R., 1999).

Dados a, b ∈ Z, b>0, siempre se hallarán q, r∈Z tales que,

$$a = bq + r, 0 \leq r \leq b \quad (5)$$

El conjunto S = {a – b_s | s∈Z, a – b_s >= 0}, es no vacío. Así que S contiene un elemento menor; digamos *r=a–bq*. Por condición *r >0*. Suponiendo que *r >= b*, se obtendría el elemento *r – b = a – b (q + 1)* ∈S, menor que r. Esta contradicción sólo se resuelve cuando *r < b.*

Este razonamiento, da el algoritmo para hallar al cociente *b* y al residuo *r* en un número finito de pasos. El algoritmo de división en Z se emplea para otra definición del m.c.d., y, en consecuencia, del m.c.m., si se toma en consideración que m.c.d. (n, m) {m.c.d.(n, m)} = nm.

Precisamente, dados los números enteros *n, m,* conjuntamente no nulos, se tiene que J = {nu + mv | u, v∈Z}. Ahora bien, J es el menor elemento positivo $d = nu_0 + mv_0$. Utilizando el algoritmo de la división, escribimos *n = dq + r, 0 <= r < d*. Habiendo elegido *d*, la lógica de

$$r = n - dq = n - (nu_0 + mv_0)q = n(1 - u_0q) + m(-v_0q) \in J \quad (6)$$

Lleva a la igualdad *r = 0*. Así que d|n (Kostrikin A.I, 1983).

Aplicando el algoritmo de la división *a, b,* y *r* se tiene que $b = rq_1 + r_1$ con $0 <= r_1 > r$. Si $r_1 = 0$, entonces *r* es el m.c.d. de *b* y *r*. Si $r_1 \neq 0$, entonces $(b,r)=(r,r_1)$ y ahora el problema de encontrar el m.c.d. de *b* y *r* se ha reducido a encontrar el mcd de *r* y r_1. Procediendo de esta forma, se obtiene lo siguiente:

$$a = bq + r \text{ con } 0 <= r > b$$
$$b = rq_1 + r_1 \text{ con } 0 <= r_1 > r$$
$$r = r_1q_2 + r_2 \text{ con } 0 <= r_2 > r_1$$
$$r_1 = r_2q_3 + r_3 \text{ con } 0 <= r_3 > r_2$$
$$r_j = r_{j+1}q_{j+2}+r_{j+2} \text{ con } 0 <= r_{j+2} < r_{j+1}$$

Ya que los r_j forman un conjunto decreciente de enteros no negativos, debe existir un r_{n+1} igual a cero. Por lo tanto:

$$r_{n-2} = r_{n-1}q_n + r_n \text{ con } 0 <= r_n < r_{n-1} \quad (7)$$
$$r_{n-1} = r_nq_{n+1} \quad (8)$$

así se tiene que $r_n = (a, b) = (b, r) = (r, r_1) = ...= (r_{n-1}, r_n)$ y por lo tanto el m.c.d. de *a* y *b* es r_n (Cárdenas y col., 1985).

B. Ecuaciones Diofantinas y Congruencias

En el apartado anterior se habló sobre el algoritmo de Euclides y su aplicación para el cálculo del mcd de una colección de números enteros. En este punto se mostrará la aplicación del algoritmo de Euclides para la solución de ecuaciones diofánticas (diofantinas) lineales en dos variables.

Sean *a, b* y *c* números enteros para todo $a \neq 0$ y $b \neq 0$, una ecuación lineal de la forma

$$ax + by = c \quad (9)$$

Con *x, y* números enteros, se llama ecuación diofántica (diofantina) lineal en dos variables. La ecuación diofántica lineal *ax + by = c* tiene solución si y sólo si *d | c* donde *d = (a, b)*.

Se tiene que si *d = (a, b), d | x, y* x_0, y_0 es una solución particular de la ecuación diofántica lineal *ax+by=c*, entonces toda solución *x*, *y* está dada por las ecuaciones $x=x_0+(b/d)t$, $y=y_0-(a/d)t$ para todo *t* perteneciente al conjunto de los números enteros.

Sustituyendo se tiene que:

$$a\,(x_0 + (b/d)t) + b(y_0 - (a/d)t) = ax_0 + (ab/d)t + by_0 - (ab/d)t = ax_0 + by_0 = c \quad (10)$$

Ya que x_0, y_0 es una solución particular de $ax+by=c$, con lo cual se concluye que x, y son en realidad soluciones de $ax + by = c$ (Kurosch, 1981).

Ahora bien, existe un concepto frecuentemente usado para resolver problemas de teoría de números que depende de las propiedades de los residuos que se obtienen al dividir dos números enteros positivos.

Sean a, b, m pertenecientes al conjunto de los números enteros, con $m>0$, se dice que a es congruente con b módulo m, lo cual se escribe como

$$a \equiv b \pmod m \quad (11)$$

Si $m \mid a\text{-}b$, al número m se le llama módulo de la congruencia. En caso contrario se dice que a y b son incongruentes módulo m. Cabe mencionar que la congruencia es una relación de equivalencia, ya que es reflexiva, simétrica y transitiva. Se tiene también que dos enteros a y b dejan el mismo residuo al dividirlos entre un entero positivo m si y solo si $a \equiv b \pmod m$ (Pettofrezzo y Byrkit, 1972).

Como se ha visto, los espacios lineales aritméticos, el algoritmo de Euclides, las ecuaciones diofánticas y las congruencias están íntimamente relacionados, y son la base de la obtención de matrices inversas modulares, mismas que se usan en el criptosistema simétrio Hill Cipher.

2. DESARROLLO

No todas las matrices cuadradas tienen inversa modular con cierto número. Existe una condición, y es la siguiente. Si el máximo común divisor (MCD) del valor absoluto de la determinante de la matriz y el módulo es igual a uno, entonces esa matriz con ese módulo si tiene una inversa modular asociada. Pero por el contrario, si el resultado del MCD es diferente a uno o mayor a uno, esa matriz con ese módulo no tiene una inversa modular asociada. Esto es que si $(MCD(|det(K)|, m) = 1)$, entonces la matriz si tiene inversa modular con dicho módulo. Sin embargo, si 'm' es primo, entonces, el MCD entre ambos elementos siempre será igual a 1. Esto garantiza la invertibilidad. He aquí un teorema encontrado.

Ahora bien, el cálculo de la inversa modular involucra la forma escalonada y reducida por renglones (Grossman, 2008), el módulo euclidiano y el algoritmo extendido de Euclides, además del producto entre dos matrices para comprobar que $(KK^{-1}) \bmod m = (K^{-1}K) \bmod m = I$, donde K representa la matriz-llave de 3 x 3, K^{-1} la inversa modular de la matriz-llave, e I representa la matriz identidad. Estas operaciones corresponden a los espacios lineales aritméticos.

Los pasos del método Gauss-Jacques son los siguientes:

1. Determinar el tamaño de la matriz-llave (K).
2. Generar la matriz-llave (K) con números aleatorios.
3. Seleccionar un valor modular 'm' que sea un número primo.
4. Escribir la matriz identidad al lado derecho de la matriz-llave considerada.
5. Encontrar un número que multiplicado por el $k_{11} \pmod m$ es igual a 1. Es decir, $k_{11} \pmod m = 1$ ó $k_{11}x = 1 \pmod m$. Se pueden encontrar una infinidad de soluciones para 'x'. Se puede aplicar el algoritmo extendido de Euclides de manera formal, o bien el método de la tabulación y el valor de verdad para la condición.

6. Generalizar la expresión que será aplicada a todo el renglón. Podemos escribir R_{nx} *(mod n)* = R_n. Donde R_n es el n-renglón. Se aplica.

7. Una vez que se han transformado los números en el n-renglón, se usa la forma escalonada y reducida por renglones (FERR).

a) En cada renglón que no sea enteramente de ceros, el elemento más a la izquierda que no es cero, será 1, usando el paso 6.

b) Cada columna que contiene el número pivote 1, deberá constar de ceros en los demás elementos de esa columna.

c) Todos los números negativos resultantes, deberán ser transformados a números naturales usado el módulo Euclidiano.

d) El pivote 1 en cada renglón, deberá encontrarse a la izquierda del pivote 1 de los renglones debajo.

e) Leer la matriz-llave del lado derecho. Esa es la inversa modular buscada, necesaria para desencriptar.

f) Multiplicar ambas matrices-llave y aplicar (mod m) al resultado. Se deberá obtener la matriz identidad (I). Este paso es como comprobación que el usuario quisiera realizar por su propia decisión.

Podemos simbolizar a la matriz inversa modular como $K^{-1}m$.

Para mostrar la aplicación de los pasos, a continuación se mostrará un ejemplo. En este caso se trabaja con un 'm' no primo, ya que satisface la condición de invertibilidad. Se puede usar cualquier matriz-llave, se seleccionó la mostrada a continuación, con el fin de acelerar la escritura del presente trabajo, y hacer llegar el método lo antes posible a la comunidad científica y tecnológica.

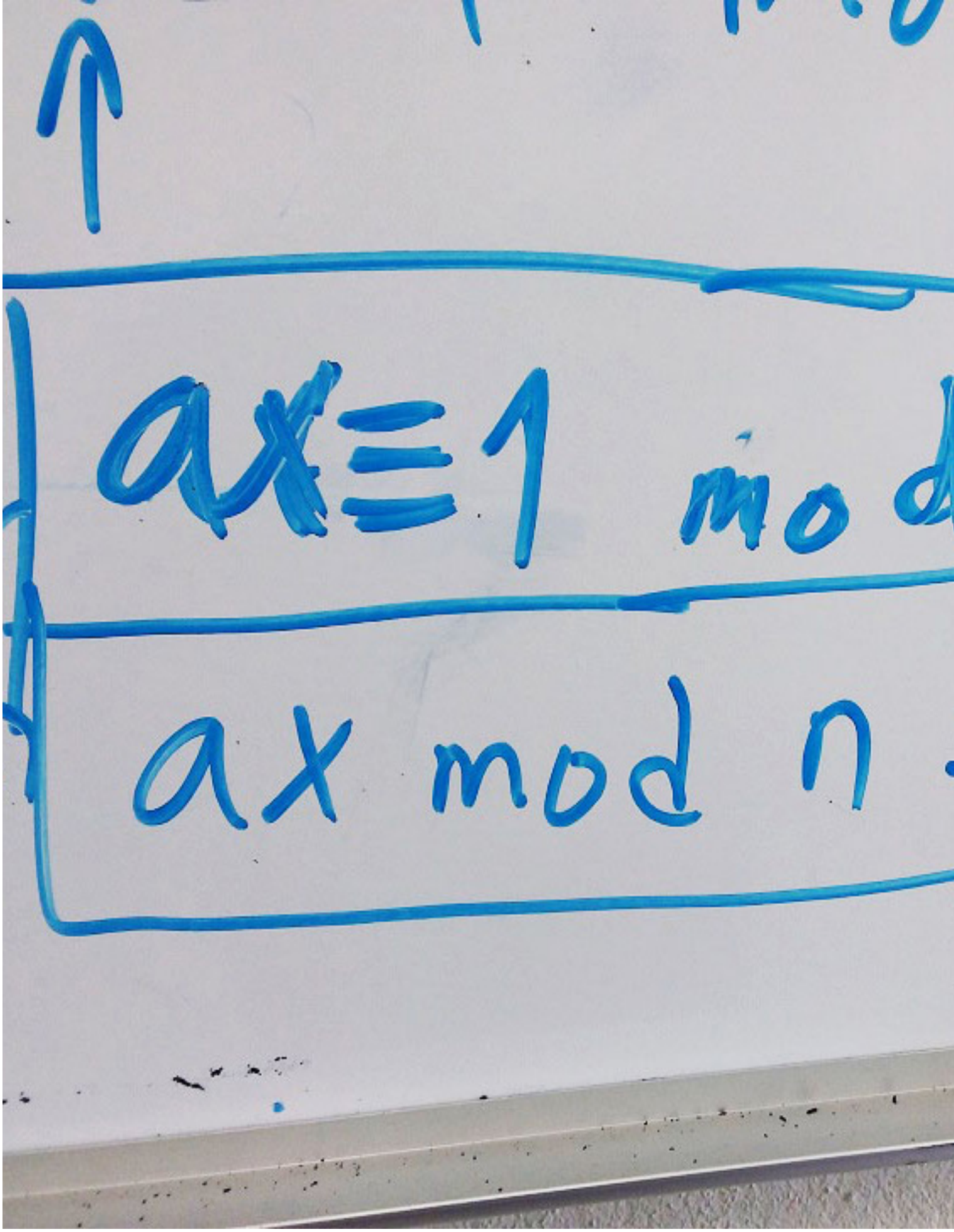
$$\left|\begin{array}{ccc|ccc} 11 & 14 & 21 & 1 & 0 & 0 \\ 9 & 17 & 10 & 0 & 1 & 0 \\ 4 & 10 & 17 & 0 & 0 & 1 \end{array}\right|$$

Teniendo la matriz aumentada, se procede a transformar el elemento a11 que es 11 en 1. Para esto se tiene que *11x mod 256 = 1*. Se tiene que encontrar el valor de *x*. Usando la ecuación de *b=pq+r,* se tiene que *11x = 256q + 1*. Despejando *x*, tenemos que *x = ((256q) + 1)/11*. Se tiene una ecuación lineal con dos incógnitas. Esto quiere decir que *x* puede tomar una infinidad de valores para que se cumpla la condición. Si tabulamos *x* en función de *q*, se obtiene:

q	x
1	23.36
2	46.63
3	69.90
.	.
.	.
.	.
7	163

Se puede observar, que cuando *q* toma el valor de 7, *x* es igual a 163. Entonces se realiza la tabulación hasta encontrar el primer valor entero. Esa es una solución. Pero he dicho que *x* puede tomar una infinidad de valores, así que otras soluciones son x = 163, 419, 675, 931, 1188, ..., ∞. Esta secuencia de números sigue un patrón. Este patrón es que al primer valor de *x* encontrado, sumamos el módulo que es igual a 256. Al número resultante volvemos a sumar el módulo. De esta forma se puede proceder hasta el infinito. Cualquiera de estos valores se pueden usar para cumplir con la condición necesaria. Para este ejemplo usemos el primer valor de *x*, que es 163.

Existe otra manera más formal de encontrar uno de los valores de *x*. Esto es usando el algoritmo extendido de Euclides. Se procede de la siguiente forma: Se usa el módulo y el elemento a transformar


ax≡1 mod
ax mod n

en un primer acercamiento. Tenemos que:

256 = 11(23) + 3
11 = 3(3) + 2
3 = 2(1) +1
2 = 1(2) + 0

Ahora bien, se realiza:

256-11(23) = 3
11-3(3) = 2
11-[256-11(23)](3) = 2
11-[256(3)-11(69)] = 2
11+256(-3)+11(69) = 2
11(70) + 256(-3) = 2

Se tiene que:

3-2(1) = 1
[256-11(23)]-[11(70)+256(-3)] = 1
256+11(-23)+11(-70)+256(3) = 1
256(4) + 11(-93) = 1

Por lo tanto, $x = -93$.

Las demás soluciones de *x*, se pueden encontrar con

$$x = x_0 + (b/d)t \quad (12)$$

Como d = m.c.d. (a, b) = 1, entonces se tiene que

$$x = x_0 + bt \quad (13)$$

Recordemos que *a* y *b* son coprimos.

El valor de *t*, puede ser cualquier número entero.

Así,

x = -93 + 256(1)
x = 163.

Corresponde a otro valor de la infinidad de soluciones de *x*.

Se puede encontrar también el valor de *q*. Esto se realiza también usando ecuaciones diofantinas. Sabiendo que y_0 es igual a 4, entonces

$q = -y_0 + (a/d)t$

Como d = m.c.d. (a, b) = 1, entonces se tiene que

$q = y_0 + at$

donde t puede ser cualquier entero. Así que

q = -4 + 11 (1)
q = 7.

Se comprueba sabiendo que

x = (256q + 1)/11
x = (256(7) + 1)/11
x = 163.

Es una de la infinidad de soluciones.

Para este ejemplo se usará el valor de 163. Tenemos *R1(163) mod 256 = R1. R1* se refiere al primer renglón de la matriz. Efectuando esta operación, la matriz queda:

1	234	95	163	0	0
9	17	10	0	1	0
4	10	17	0	0	1

Se ha modificado el primer renglón. Ahora se usa el pivote para reducir los elementos de su columna, que son el 9 y el 4. Así que se emplea la fórmula *(R1(-9) + R2) mod 256 = R2, y (R1(-4) + R3) mod 256 = R3.* Al hacer esto se obtiene la matriz:

1	234	95	163	0	0
0	215	179	69	1	0
0	98	149	116	0	1

Se han modificado los renglones 2 y 3. El siguiente

paso es escalonar, es decir, transformar el elemento a_{22} que es 215 en 1. Se procede de la misma forma hasta escalonar y reducir la matriz. Al desarrollar el método para este ejemplo, se obtiene la matriz:

$$\left|\begin{array}{ccc|ccc} 1 & 0 & 0 & 131 & 28 & 153 \\ 0 & 1 & 0 & 49 & 89 & 113 \\ 0 & 0 & 1 & 106 & 182 & 3 \end{array}\right|$$

La matriz inversa modular con módulo igual a 256 es:

$$\left|\begin{array}{ccc} 131 & 28 & 153 \\ 49 & 89 & 113 \\ 106 & 182 & 3 \end{array}\right|$$

Para comprobar que efectivamente esta matriz corresponde a la inversa modular, se procede a multiplicar por la matriz original de la forma antes mencionada $(KK^{-1}) \bmod 256 = I$.

$$\left|\begin{array}{ccc} 11 & 14 & 21 \\ 9 & 17 & 10 \\ 4 & 10 & 17 \end{array}\right| \left|\begin{array}{ccc} 131 & 28 & 153 \\ 49 & 89 & 113 \\ 106 & 182 & 3 \end{array}\right| = \left|\begin{array}{ccc} 4353 & 5376 & 3328 \\ 3072 & 3585 & 3328 \\ 2816 & 4096 & 1793 \end{array}\right|$$

Aplicando el módulo igual a 256 a cada elemento de la matriz resultante del producto se obtiene:

$$\left|\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right|$$

Que corresponde a la matriz identidad. Esto significa que la matriz inversa modular que encontramos es correcta.

2. DISCUSIÓN

Sobre la complejidad computacional se tiene que es un polinomio de grado 3. Dicho polinomio es: $((x^3)+((x^2-x)/2)+(y^2+y))$. Es una función de dos variables cuya gráfica corresponde a las tres dimensiones. La variable 'x' corresponde al tamaño de la matriz cuadrada de n x n, esto es, a 'n'. Mientras que la variable 'y' corresponde al valor modular *(mod m)* seleccionado, esto es, a 'm'. Se tiene una función $z = f(x,y)$ como dependiente de 'x', y 'y'. Se puede expresar también como: $((n^3)+((n^2-n)/2)+(m^2+m))$, quedando la función como $c=f(n, m)$; donde 'c' se refiere a la complejidad computacional.

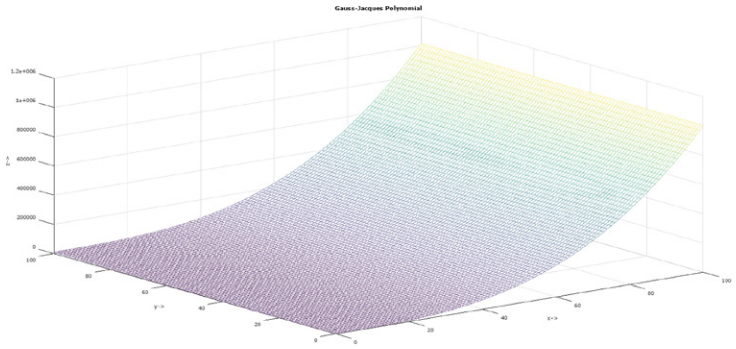


Figura 1. Polinomio del método Gauss-Jacques con [x, y]=(0:100).

Se observa que es muy eficiente su comportamiento según crecen las variables x, y. Es eficiente y óptimo en computadoras. Se recomienda para procesamiento en tarjetas o dispositivos móviles. Un servidor puede sin duda alguna procesar el método con matrices n x n de gran tamaño, asegurando así, la seguridad de los datos encriptados. La figura 1 se programó en el software libre GNU-Octave.

Se observa también que con una matriz cuadrada de tamaño 100 x 100 que corresponde a 10,000 elementos, se procesa su inversa modular con el método Gauss-Jacques de manera eficiente. Se puede tener una idea de la tendencia de la función al aumentar 'x' para determinado 'y'. La cantidad de operaciones que ejecutaría la computadora se observa en el eje de las z's. Teniendo en cuenta que un procesador puede ejecutar millones de operaciones aritméticas por segundo, se sabe que es muy eficiente el tiempo de cómputo requerido para ciertas matrices con determinado valor modular.

TEOREMA: Para toda matriz cuadrada de tamaño 'n', compuesta de números naturales; y todo valor modular 'm' primo, se encontrará una inversa modular asociada con el método Gauss-Jacques.

4. CONCLUSIONES

Una matriz-llave candidata puede tener una infinidad de inversas modulares por cada valor 'm' que se maneje. Así mismo, una matriz-llave tiene solo una inversa modular para ese módulo 'm' si es invertible. Una matriz-llave puede no tener inversa modular para cierto valor de 'm', si 'm' no es primo.

Según la pendiente 'm' de la recta, existen una infinidad de puntos (x, y) en el plano R2, que conformar la línea. Por lo tanto, cada par (x, y) puede ser usado para resolver el sistema y proseguir con el método. El obvio deducir que el resultado siempre será el mismo no importando el valor de 'x' que se use. Una observación importante que me gustaría puntualizar, es que el 'q' de la divisibilidad Euclidiana toma el valor de 'y' multiplicado por '-1', esto es: q = -1(y). Esto debido a las ecuaciones diofánticas o diofantinas de las que se ha hablado en el presente trabajo.

Como se ha mencionado, para garantizar que cualquier matriz aleatoria es invertible modularmente, solo es necesario seleccionar como valor modular un número primo. De esta forma, el máximo común divisor entre el valor absoluto de la determinante y el valor modular, siempre será uno. Para calcular la determinante de una matriz cuadrada de tamaño n x n de forma eficiente computacionalmente hablando, se tiene que usar la factorización LU. Se multiplican los elementos de la diagonal principal de la matriz U encontrada, y el resultado, es el determinante de la matriz.

Recordemos que un teorema es una proposición cuyo valor lógico de verdad ha sido demostrado. Pues se tiene que la inversa modular, de la inversa modular es igual a la matriz original. Para algunas matrices, este ejercicio no es inmediato, es decir, se tiene que intercambiar renglones, o bien, transponer la matriz. Este teorema se cumple para toda matriz invertible, pero, según los elementos que la componen y sus propiedades, crece un tanto la complejidad computacional para llegar a la original. Obviamente, si se transpuso, al terminar con el método, se tiene que volver a acomodar según la transposición.

La obtención de la inversa modular de una matriz cuadrada involucra diversos temas correspondientes a Teoría de números, álgebra superior y álgebra lineal.

La obtención de la inversa modular de una matriz cuadrada puede ser programada en un algoritmo preciso, definido y finito.

Uno de los usos de las matrices inversas modulares se da en la criptografía simétrica. Específicamente el algoritmo Hill Cipher.

El proceso de desencriptación en fundamental un criptosistema. Por más seguro que sea un algoritmo para encriptar un conjunto de datos, si no se pueden recuperar, dicho algoritmo es inservible.

Si usamos la teoría de la combinatoria, y cada llave no es necesariamente un cuadrado latino, entonces se permite la repetición. Por cada elemento de la matriz en base a la cantidad de dígitos que lo componen y usando el principio de la multiplicación dentro de este contexto, la cantidad de llaves diferentes que se pueden formar de tamaño n x n con 1, 2, 3, ó más dígitos para cada elemento, prácticamente tiende a infinito. Se puede expresar como $n^2(m^n)$, donde 'n' corresponde al número de renglones o columnas, y 'm' a la cantidad de números diferentes que pueden usarse para cada casilla o elemento k_{ij} dentro de la matriz-llave candidata K. Se pueden trabajar con llaves

desechables, cambiando la misma cada tiempo *t* definido, según las condiciones. De esta forma, la ventana de tiempo en la que el Hacker procura desencriptar se reduce, haciéndolo prácticamente imposible.

Se han hecho experimentos en el rendimiento computacional del algoritmo en dispositivos móviles, programado en el lenguaje de programación orientado a objetos Java para Android. El tiempo de procesamiento es relativamente corto para matrices grandes.

Actualmente se está probando en computadoras personales programado en el lenguaje C++. Se han hecho experimentos en computadoras de gama media con matrices-llave de un millón de elementos y el tiempo de respuesta es alentador.

Se contempla de trabajo futuro, realizar experimentos utilizando cómputo paralelo, y medir el rendimiento computacional para matrices o llaves donde n > 1000, y m>3.

Así mismo se contempla como una nueva propuesta en criptografía cuántica.

Resumen Curricular

Fausto Abraham Jacques García

Es un profesor- investigador y candidato a doctor de la criptografía simétrica, matemáticas aplicadas educativas y tópicos selectos de la Inteligencia Artificial. Posee diversos artículos y ponencias científicas en Estados Unidos de América (USA), Cuba y México

Referencias Bibliográficas

Cárdenas, H., y cols. (1985). *Algebra Superior.* México: Trillas.

GNU Octave, versión 4.2.1, copyright © 2017, John W. Eaton and others.

Johnsonbaugh, R. (1999). *Matemáticas Discretas.* Chicago: Prentince Hall.

Grossman, S., (2008). *Álgebra Lineal* [Linear Algebra], 6ta. Ed., Mexico, DF: McGraw-Hill.

Kostrikin Alexei I. (1983). *Introducción al Álgebra.* Moscu: Mir.

Kurosch A.G. (1981). *Curso de Álgebra Superior.* Moscú: Mir.

Pettofrezzo, A.J., y Byrkit, D.R. (1972). *Introducción a la Teoría de los Números.* Madrid: Prentice Hall.