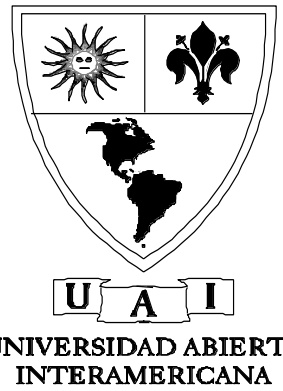


UNIVERSIDAD ABIERTA INTERAMERICANA

Carrera: Licenciatura en Matemática

Algoritmo criptográfico para descifrar el protocolo de intercambio de claves HK17

Autor: Sergio Bernstein

Directora de Tesis: Dra. Samira Abdel Masih

Tesis presentada para optar al título de

Licenciado en Matemática

- Junio 2021 -

Firmas del jurado

Resumen

La Criptografía es la ciencia que tiene por objetivo crear algoritmos para garantizar la seguridad de la información que se transmite por un determinado canal. Gracias a la Criptografía, se pueden generar claves para que la información permanezca protegida y evitar que personas no autorizadas tengan acceso a ella.
El primer algoritmo criptográfico que permitió intercambiar claves a través de un canal público fue el *Protocolo de Intercambio de Claves de Diffie-Hellman* ([1]). Presentado en *1976,* sentó las bases para el surgimiento de lo que hoy se conoce como Criptografía de Clave Pública o Asimétrica. Si bien este algoritmo es criptográficamente seguro, precisa de ciertos recursos computacionales potentes, como por ejemplo, bibliotecas de precisión extendida.
En el año *2015* Jorge Kamlofsky y Pedro Hecht modificaron el *Protocolo de Diffie-Hellman* empleando una estructura algebraica no conmutativa: el anillo de cuaterniones ([3]).
Y en *2017*, ambos autores optimizaron aún más este algoritmo aplicando una estructura algebraica más amplia: los octoniones. Esto dio origen al llamado *Protocolo HK17* ([4]).
Estos métodos criptográficos diseñados por Kamlofsky y Hecht otorgan un gran beneficio: pueden ser ejecutados en procesadores de bajo poder computacional y memoria RAM reducida, como por ejemplo, en tarjetas inteligentes o teléfonos celulares.
Fueron considerados criptográficamente seguros, hasta que en el año *2019* científicos de la Academia China de Ciencias: Haoyu, Renzhang, Qutaibah, Yanbin, Yongge y Tianyuan, propusieron un algoritmo de ataque para descifrar la clave generada por el Protocolo HK17.
En este trabajo analizaremos la publicación presentada por dichos autores chinos, citada en la Referencia [5]. Veremos que aplicando ciertas propiedades aritméticas de los octoniones, se podrá descubrir de manera efectiva la clave generada por el Protocolo HK17, como así también la del algoritmo criptográfico que emplea cuaterniones.

Palabras claves:

Criptografía, Diffie-Hellman, Protocolo HK17, Aritmética Modular, Cuaterniones y octoniones.

Índice general

Capítulo 1

Nociones básicas de Criptografía

Desde que el ser humano tuvo la necesidad de comunicarse con una o más personas, ha buscado la forma transmitir ideas, pensamientos, dando origen a lo que hoy se conoce como *modelo de comunicación*.
Pero para que exista un *modelo de comunicación básico*, es necesario que el emisor (origen) proporcione un mensaje o texto, a trasmitir por un medio a un receptor (destinatario), como se muestra en la siguiente Figura:

Figura 1.1: Modelo de comunicación básico.

En muchos casos la comunicación no sólo requería transmitir información, sino que además se precisaba que esa información no fuera conocida por personas ajenas a ella.
Por este motivo surgió la tarea de buscar métodos o técnicas para ocultarla, dando origen a lo que hoy se conoce como Criptografía. Su nombre proviene del griego "*kryptos*" que significa oculto, y "*graphia*", que significa escritura. Su definición es la siguiente:

> ***Definición 1.1: Criptografía***
>
> *La Criptografía es la ciencia que se ocupa de crear algoritmos para ocultar mensajes y de este modo, evitar que sean leídos por personas no autorizadas.*

La Criptografía se compone de dos pasos: ***Cifrado*** y ***Descifrado***.

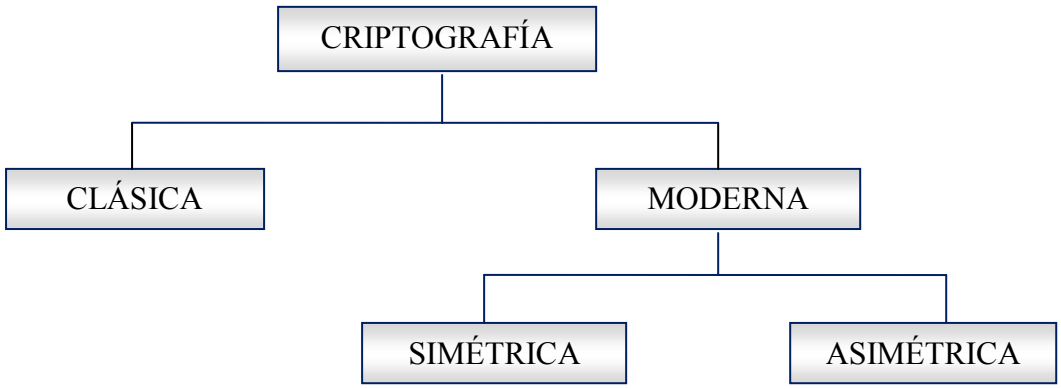
Cifrado: Consiste en convertir un mensaje (texto llano) a un texto cifrado.

Descifrado: Consiste en recuperar el mensaje original a partir del texto cifrado.

El cifrado lo realiza el emisor del mensaje. Mientras que el descifrado lo lleva a cabo el receptor del mensaje.
Para crear los algoritmos que permitan cifrar o descifrar los mensajes, la Criptografía se vale de diversas ramas de la Matemática, entre ellas, la Matemática Discreta y el Álgebra.

Clasificación de la Criptografía

La Criptografía se clasifica básicamente según el siguiente diagrama que mostramos a continuación:



Explicaremos brevemente el significado de cada una de estas criptografías:

La Criptografía Clásica es la que se empleó desde la antigüedad hasta la primera mitad del siglo XX. También puede entenderse como la Criptografía no computarizada o no digitalizada.
Aplicaban diversos métodos para ocultar mensajes, que sólo podían leer personas de mucho prestigio como reyes y jefes militares. En muchos casos fue utilizada para la comunicación en las guerras. Como ejemplo de Criptografía clásica podemos citar a la *Escítala*, que fue el primer sistema criptográfico de la historia. Fue utilizada por los espartanos en el siglo V a.C. para el envío de mensajes escritos. Está formada por dos varas de igual grosor y de una tira de cuero o papiro sobre la cual se escribe el mensaje. Los detalles de su funcionamiento están explicados en la Referencia [7].

Figura 1.2: La Escítala. Fuente: http://ojoscuriosos.com/la-escitala/.

La Criptografía Moderna utiliza algoritmos matemáticos para cifrar y descifrar mensajes. Se inició después de tres hechos importantes: el primero, en *1940*, con la publicación por parte de Shannon de la "*Teoría de la Información*"; el segundo, con la aparición en *1974* del sistema de cifrado DES (Data Encryption Standard) y finalmente, en *1976*, con el estudio realizado por Whitfield Diffie y Martin Hellman referente a la aplicación de funciones matemáticas a un modelo de cifrado, denominado "C*ifrado de Llave Pública"*. De acuerdo a las técnicas o métodos empleados para cifrar los mensajes, la Criptografía Moderna se puede clasificar en: ***Criptografía Simétrica*** y ***Criptografía Asimétrica.***

Criptografía Simétrica: Cuando el emisor y receptor usan la misma clave para cifrar que para descifrar. Esto supone un grave problema a la hora de realizar el intercambio entre el emisor y el receptor, dado que si una tercera persona estuviese escuchando el canal, podría capturar la clave, siendo inútil el cifrado.
Es importante que la clave sea difícil de descubrir. En la actualidad, con la capacidad computacional disponible, se puede obtener la clave en cuestión de minutos u horas. Por esta razón este tipo de Criptografía ya no es segura.

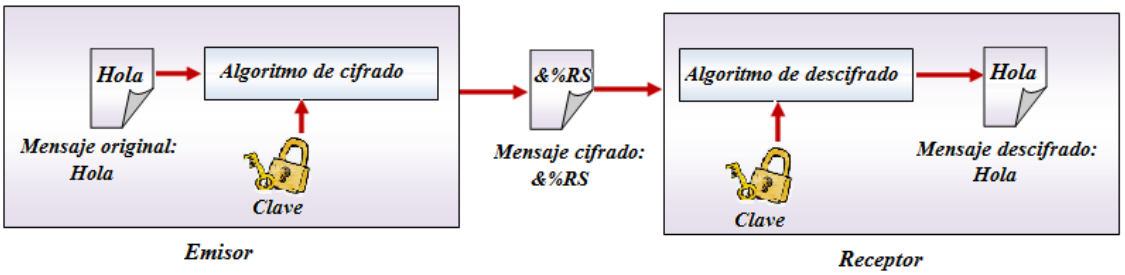


Figura 1.3: Criptografía Simétrica

Ejemplos de Criptografía Simétrica son: El Método de Julio César, el Método Lineal ó de Julio César Mejorado y el Método de las Digrafías. Los detalles del funcionamiento de estos métodos se encuentran en las Referencias [6] y [7].

Criptografía Asimétrica: Cuando la clave que utiliza el emisor para cifrar es distinta a la que utiliza el receptor para descifrar. Este tipo de Criptografía se basa en el uso de dos claves distintas:

- ***Clave pública***
- ***Clave privada***

En un sistema de comunicación asimétrico, la idea es que cada usuario que participa en esta comunicación cifrada genere su propia clave, que será la *clave privada,* la cual no podrá ser revelada. Mientras que la *clave pública* se distribuye al resto del equipo y puede ser conocida por todos.
Este tipo de Criptografía ofrece un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros, puesto que únicamente viaja por el canal la *clave pública*. Sin la *clave privada* (que no es deducible a partir de la *clave pública*) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.

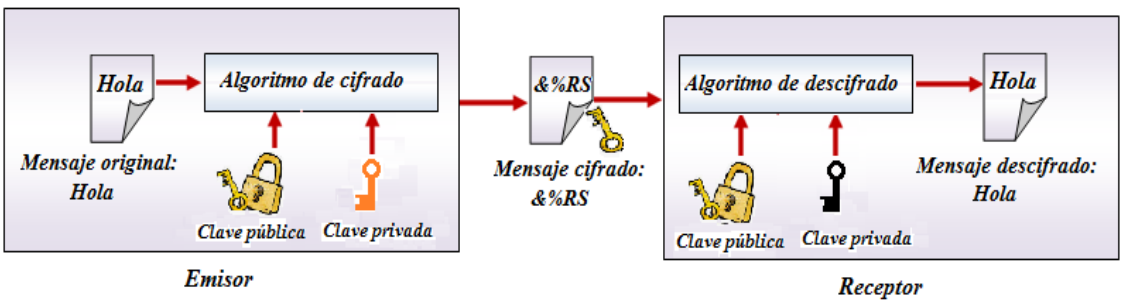


Figura 1.4: Criptografía Asimétrica

Algunos ejemplos de criptografía asimétrica son: Algoritmo de Diffie-Hellman y las variantes propuestas por Kamlofsky y Hecht. Estos algoritmos los veremos en los Capítulos *3* y *4*.

Finalizaremos este capítulo con un ejemplo de Criptografía Clásica: El método de Polybios.

El método criptográfico de Polybios

A mediados del siglo II a.C., el historiador griego Polybios (*200-118* a.C.) creó un método criptográfico que consistía en hacer corresponder a cada letra del alfabeto un par de letras que indicaban la fila y la columna en la cual aquélla se encontraba, en un recuadro de $5 \times 5 = 25$ caracteres. En la Figura *1.5* mostramos una tabla de Polybios adaptada al alfabeto latino:

	A	***B***	***C***	***D***	***E***
A	***A***	***B***	***C***	***D***	***E***
B	***F***	***G***	***H***	***I,J***	***K***
C	***L***	***M***	***N***	***O***	***P***
D	***Q***	***R***	***S***	***T***	***U***
E	***V***	***W***	***X***	***Y***	***Z***

Figura 1.5: Tabla de Polybios

Acorde con este método, la letra A se cifrará como AA, la H como BC y así sucesivamente. El método fue genial en su época, pero en la actualidad resulta obsoleto ya que, con los recursos computacionales actuales, los mensajes cifrados de Polybios pueden descubrirse fácilmente.

Ejemplo 1.2

Aplicando la Tabla de Polybios, cifrar el mensaje:

QUE GENIAL IDEA

Solución

Al aplicar la Tabla de Polybios de la Figura *1.5*, obtenemos que el texto cifrado es

DADEAE BBAECCBDAACA BDADAEAA

Capítulo 2

Nociones matemáticas básicas

En este capítulo expondremos las nociones matemáticas que utilizaremos en este trabajo. Comenzaremos definiendo la Aritmética Modular y sus propiedades, un tema fundamental para comprender los algoritmos criptográficos que desarrollaremos en los Capítulos 3 y *4*. Posteriormente definiremos las estructuras algebraicas que emplearon los autores Kamlofsky y Hecht para modificar el *Protocolo de intercambio de claves de Diffie-Hellman*: el anillo de cuaterniones y los octoniones.

1. Aritmética Modular

La Aritmética Modular es la parte de la Aritmética que opera con números enteros, considerando el resto de la división de dichos números enteros por un número natural "*n*" fijo, llamado "*el módulo de n*".
Esta rama de la Matemática fue creada por Gauss (*1777-1855*) para resolver, de una manera más sencilla, las ecuaciones diofánticas. Estas ecuaciones fueron planteadas por Diofanto de Alejandría (*200-284*), las cuales son de la forma:

$$a\,x + b\,y = c$$

Donde $a, b, c \in \mathbb{Z}$. Incógnitas: $x, y \in \mathbb{Z}$

La Aritmética Modular utiliza la divisibilidad y congruencia como conceptos básicos. Estas definiciones las damos a continuación.

Definición 2.1: Divisibilidad

Sean a y b $\in \mathbb{Z}$ *con* $b \neq 0$. *Se dice que "b" divide a "a" y se escribe* $b \mid a$ *si a = k. b para algún* $k \in \mathbb{Z}$ *. O equivalentemente, si al dividir a por b, el resto da 0.*

Definición 2.2: Congruencia

Dado un número natural n>1 y dos números a y $b \in \mathbb{Z}$. *Se dice que a es congruente con b módulo n y se indica*

$$a \equiv b \pmod{n}$$

Si $n \mid (b-a)$ ó $n \mid (a-b)$

Ejemplo 2.3

1) $17 \equiv 2 \pmod{3}$ pues $3 \mid (17-2)$

2) $13 \not\equiv 6 \pmod{5}$ pues $5 \nmid (13-6)$

La siguiente Proposición enumera ciertas propiedades de la congruencia que aplicaremos en esta tesis:

Proposición 2.4: *Sean* $a,b,c \in \mathbb{Z}$ *. Entonces*

1) *Propiedad Reflexiva:*
$$a \equiv a \pmod{n}$$
2) *Propiedad Simétrica:*
$$\forall a,b \in \mathbb{Z} \text{ , si } a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$$
3) *Propiedad Transitiva:*
$$\forall a,b,c \in \mathbb{Z} \text{ , si } a \equiv b \pmod{n} \wedge b \equiv c \pmod{n}) \Rightarrow a \equiv c \pmod{n}$$
4) $\forall a \in \mathbb{Z}$, $a \equiv 0 \pmod{n} \Leftrightarrow n \mid a$
5) $\text{Si } a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a.c \equiv b.d \pmod{n}$
6) $\text{Si } a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a+c \equiv b+d \pmod{n}$
7) $\text{Si } a \equiv b \pmod{n} \wedge c \neq 0 \Rightarrow a.c \equiv b.c \pmod{n}$
8) $\text{Si } a \equiv b \pmod{n} \wedge k \in \mathbb{N} \Rightarrow a^k \equiv b^k \pmod{n}$
9) $a \equiv b \pmod{n} \Leftrightarrow a \wedge b$ *tienen el mismo resto en la división entera por n*
10) $a \equiv r_a \pmod{n}$ *donde* r_a *es el resto de la división entera de a por n*
11) $a \equiv n+a \pmod{n}$

Demostración

Véase Referencia [8]. ■

El conjunto $\mathbb{Z}_n$

De la Proposición *2.4* inciso *10*), se sabe que si $a \in \mathbb{Z}$ y *n* es un natural mayor que *1*, entonces $a \equiv r_a \pmod{n}$, donde r_a es el resto de la división entera de *a* por *n*. Esto permite clasificar a los números enteros según el resto de su división entera por *n*. Sabemos que los posibles restos son *0, 1, .., n -1* . Este hecho da lugar a la siguiente:

Definición 2.5: El conjunto $\mathbb{Z}_n$

Si n es un número natural mayor que 1, el conjunto $\mathbb{Z}_n$ *es*

$$\mathbb{Z}_n = \{ 0, 1, 2, ..., n-1 \}.$$

A dicho conjunto se le definirán ciertas operaciones, a fin de dotarlo de una estructura algebraica conveniente.

***Notación*:** utilizaremos la siguiente equivalencia: $a \equiv b \ (mod\ n) \Leftrightarrow\ a = b$ en $\mathbb{Z}_n$

Operaciones en $\mathbb{Z}_n$

Definición 2.6: Suma, Producto y Potencia en $\mathbb{Z}_n$

Sean $a, b, c \in \mathbb{Z}$. Entonces

1) Suma en $\mathbb{Z}_n$:

$$a+b=c \text{ (en } \mathbb{Z}_n) \Leftrightarrow \text{c es el resto de la división entera de } (a+b) \text{ por } n.$$

2) Producto en $\mathbb{Z}_n$:

$$a \,.\, b=c \text{ (en } \mathbb{Z}_n) \Leftrightarrow \text{c es el resto de la división entera de } (a \,.\, b) \text{ por n}.$$

3) Potencia en $\mathbb{Z}_n$: Si $n \in \mathbb{N}$ entonces:

$$a^n = \underbrace{a.\, a. \ldots . a}_{n \text{ veces}}$$

$$a^0 = 1$$

De la Definición anterior se deduce que

1) $a+b=c \text{ (en } \mathbb{Z}_n) \Leftrightarrow a+b \equiv c \ (mod\ n)$

2) $a \,.\, b=c \text{ (en } \mathbb{Z}_n) \Leftrightarrow a \,.\, b \equiv c \ (mod\ n)$

Definición 2.7: Elementos neutros para la suma y multiplicación en $\mathbb{Z}_n$

El neutro para la suma es el "0" pues $a+0=a$ (mod n) $\forall a \in \mathbb{Z}_n$

El neutro para el producto es el "1" pues $a \,.1=a$ (mod n) $\forall a \in \mathbb{Z}_n$

Definición 2.8: El opuesto de $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$, el opuesto de a es un número $b \in \mathbb{Z}_n$ tal que $a+b=0$ (mod n)

La siguiente proposición muestra como calcular el opuesto de un elemento de $\mathbb{Z}_n$

Proposición 2.9

Si $a \in \mathbb{Z}_n$ entonces su opuesto es $(n-a)$

Demostración

Véase Referencia [7]

Notación: al opuesto de a lo simbolizaremos por "$-a$".

Ejemplo 2.10

Sea $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}$. Hallar el opuesto de *5*.

Solución

En este caso, $n = 8$. Por lo tanto, el opuesto de 5 es $n - 5 = 8 - 5 = 3$.

Definición 2.11: Inverso en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$ con $a \neq 0$, el inverso de a es un número $b \in \mathbb{Z}_n$ tal que $a \,.\, b = 1$ en $\mathbb{Z}_n$

Notación: al inverso de a lo simbolizaremos por a^{-1} .

No todo elemento de $\mathbb{Z}_n$ tiene inverso. El siguiente teorema nos indica en qué casos un elemento en $\mathbb{Z}_n$ es invertible.

Teorema 2.12: Teorema de Invertibilidad

Un elemento $a \in \mathbb{Z}_n$ es invertible $\Leftrightarrow$ $mcd(a,n) = 1$

Demostración

Véase Referencia [6]. ■

Corolario 2.13: Corolario del Teorema de invertibilidad en $\mathbb{Z}_n$

Si n es primo entonces todo elemento de $\mathbb{Z}_n$ es invertible

Demostración

Véase Referencia [7]. ■

La siguiente Proposición determinará cómo calcular el inverso de un elemento en $\mathbb{Z}_n$.

Proposición 2.14

Sea $a \in \mathbb{Z}_n$ tal que a es invertible en $\mathbb{Z}_n$. Entonces su inverso es $a^{-1} = \dfrac{1 + n\ k}{a}$

para algún $k \in \mathbb{Z}$ tal que $0 \leq k \leq a \ \wedge \ \dfrac{1 + n\ k}{a} \in \mathbb{Z}$

Demostración

Véase Referencia [6]. ■

Ejemplo 2.15

Calcular los siguientes inversos, en caso que existan, en el conjunto que se indica:

1) 5^{-1} en $\mathbb{Z}_{15}$ 2) 7^{-1} en $\mathbb{Z}_{11}$

Solución

1) Como $mcd(5,15)=5\neq 1$ por el Teorema *2.12* (Teorema de Invertibilidad) resulta que 5 no tiene inverso en $\mathbb{Z}_{15}$.

2) Como $mcd(7,11)=1$ entonces 7 tiene inverso en $\mathbb{Z}_{11}$. Por la Proposición *2.14*,

$$7^{-1}=\frac{1+11k}{7}$$

Para algún $k\in\mathbb{Z}$ tal que $0\leq k\leq 7\wedge \frac{1+11k}{7}\in\mathbb{Z}$. A fin de determinar cuál es el valor de *k*, diseñamos la siguiente tabla:

k	*0*	*1*	*2*	*3*	*4*	*5*
$\frac{1+11k}{7}$	$\frac{1}{7}\notin\mathbb{Z}$	$\frac{12}{7}\notin\mathbb{Z}$	$\frac{23}{7}\notin\mathbb{Z}$	$\frac{34}{7}\notin\mathbb{Z}$	$\frac{45}{7}\notin\mathbb{Z}$	$\frac{56}{7}=8\in\mathbb{Z}$

Por lo tanto, $7^{-1}=8$ en $\mathbb{Z}_{11}$.

El siguiente programa, diseñado con el software Wolfram Mathematica *11.0*, calcula el inverso de un número en $\mathbb{Z}_n$.

```
Interpretation[{a = 10, n = 27},
 Panel[Grid[{{Style["Ingrese el número a calcular su inverso", Bold], SpanFromLeft},
    {"a=", InputField[Dynamic[a]]},
    {Style["Ingrese el valor del módulo n", Bold], SpanFromLeft},
    {"n=", InputField[Dynamic[n]]}
    }]],
 If[GCD[a, n] ≠ 1, Print["El número ", a, " no es iversible en Zn"],
  Encontrado = 0;
  k = 1;
  While[k ≤ a && Encontrado == 0,
   If[Mod[1 + n k, a] == 0, Encontrado = 1];
   k++;
  ];
  Print["El inverso de ", a, " es  ", (1 + n (k - 1))/a]
 ]
]
```

Potencias modulares

Dado $a \in \mathbb{Z}_{\geq 0}$ y $k \in \mathbb{N}$, el cálculo de la potencia modular consiste en hallar $a^k \ (mod\ n)$. Es decir, se trata de calcular el resto de la división entera entre a^k y el número *n*. Pero calcular a^k y luego efectuar la división entera para hallar el resto, se torna sumamente dificultoso si *a* es un número grande.
Además, puede producir *owerflow* (desbordamiento aritmético) en una computadora. Por esta razón presentamos el siguiente algoritmo para permitir calcular $a^k \ (mod\ n)$ de un modo más eficiente. El algoritmo se basa en el siguiente hecho:
Si se efectúa la división entera de *k* por *2*, se obtiene:

$$k = 2\left[\frac{k}{2}\right] + r$$

Donde

$\left[\frac{k}{2}\right]$: Parte entera de $\frac{k}{2}$.

r : Resto de la división $(0 \leq r \leq 1)$.

En consecuencia, $a^k = a^{2\left[\frac{k}{2}\right]+r} = \left(a^2\right)^{\left[\frac{k}{2}\right]} . a^r$

Esta expresión permite generar las siguientes sucesiones:
$\{a_0 , a_1 , a_2 ,...\} , \{k_0 , k_1 , k_2 ,...\} , \{c_0 , c_1 , c_2 ,...\} , \{r_0 , r_1 , r_2 ,...\}$

Con

$$\begin{cases} a_0 = a \\ k_0 = k \\ c_0 = 1 \\ r_0 = r \end{cases}$$

Los demás términos de las sucesiones se definen del siguiente modo, aplicando las propiedades de congruencia enunciadas en los incisos 5), 8) y 9) de la Proposición *2.4*:

$$a^k = a^{2\left[\frac{k}{2}\right]+r_0} = \left(a^2\right)^{\left[\frac{k}{2}\right]} . a^{r_0} \equiv a_1^{k_1} . c_1 = \left(a_1^2\right)^{\left[\frac{k_1}{2}\right]} . a_1^{r_1} . c_1 \equiv a_2^{k_2} . c_2 = ...$$

$$\uparrow \qquad\qquad\qquad\qquad \uparrow$$

$$\begin{cases} a_1 \equiv a^2 \ (mod\ n) \\ k_1 = \left[\frac{k}{2}\right] \\ c_1 \equiv a^{r_0} = a^{r_0} . c_0 \ (mod\ n) \end{cases} \qquad \begin{cases} a_2 \equiv a_1^2 \ (mod\ n) \\ k_2 = \left[\frac{k_1}{2}\right] \\ c_2 \equiv a_1^{r_1} . c_1 \ (mod\ n) \end{cases}$$

El proceso sigue hasta que $k_i \leq 1$ para algún i. El pseudocódigo del algoritmo lo mostramos a continuación:

Algoritmo para calcular $a^k \pmod{n}$

$a_0 = a\ ,\ k_0 = k\ ,\ c_0 = 1\ ,\ i = 1$

Mientras $k_{i-1} > 1$ *hacer:*

$a_i \equiv a_{i-1}^2 \pmod{n}$

Si k_{i-1} *es par entonces*

$c_i = c_{i-1}$

Sino $c_i = a_{i-1} \cdot c_{i-1} \pmod{n}$

Fin si

$k_i = \left[\frac{k_{i-1}}{2}\right]$

$i = i + 1$

Fin mientras

$a^k \equiv a_{i-1} \cdot c_{i-1} \pmod{n}$

Desarrollaremos un Ejemplo que ayudará a comprender este algoritmo.

Ejemplo 2.16

Calcular $126^{85} \pmod{312}$

Solución

En este caso, $a = 126$ y $k = 85$. A fin de ordenar los cálculos, diseñamos la siguiente tabla:

i	a_i	c_i	k_i
0	*126*	*1*	*85*
1	*276*	*126*	*42*
2	*48*	*126*	*21*
3	*120*	*120*	*10*
4	*48*	*120*	*5*
5	*120*	*144*	*2*
6	*48*	*144*	*1*

Los detalles de los datos que figuran en la tabla los explicamos a continuación:

Para i = 0

$a_0 = a = 126$
$c_0 = 1$
$k_0 = k = 85$

Para i = 1

$$a_1 = a_0^2 = (126)^2 = 15876 \equiv 276 \pmod{312}$$
$$c_1 = a_0 \times c_0 = 126 \times 1 = 126 \pmod{312}$$
$$k_1 = \left\lfloor \frac{k_0}{2} \right\rfloor = \left\lfloor \frac{85}{2} \right\rfloor = \lfloor 42.5 \rfloor = 42$$

Para i = 2

$$a_2 = a_1^2 = (276)^2 = 76176 \equiv 48 \pmod{312}$$
$$c_2 = c_1 = 126 \pmod{312}$$
$$k_2 = \left\lfloor \frac{k_1}{2} \right\rfloor = \left\lfloor \frac{42}{2} \right\rfloor = \lfloor 21 \rfloor = 21$$

Para i = 3

$$a_3 = a_2^2 = (48)^2 = 2304 \equiv 120 \pmod{312}$$
$$c_3 = a_2 \times c_2 = 48 \times 126 = 6048 \equiv 120 \pmod{312}$$
$$k_3 = \left\lfloor \frac{k_2}{2} \right\rfloor = \left\lfloor \frac{21}{2} \right\rfloor = \lfloor 10.5 \rfloor = 10$$

Para i = 4

$$a_4 = a_3^2 = (120)^2 = 14400 \equiv 48 \pmod{312}$$
$$c_4 = c_3 = 120 \pmod{312}$$
$$k_4 = \left\lfloor \frac{k_3}{2} \right\rfloor = \left\lfloor \frac{10}{2} \right\rfloor = \lfloor 5 \rfloor = 5$$

Para i = 5

$$a_5 = a_4^2 = (48)^2 = 2304 \equiv 120 \pmod{312}$$
$$c_5 = a_4 \times c_4 = 48 \times 120 = 5760 \equiv 144 \pmod{312}$$
$$k_5 = \left\lfloor \frac{k_4}{2} \right\rfloor = \left\lfloor \frac{5}{2} \right\rfloor = \lfloor 2.5 \rfloor = 2$$

Para i = 6

$$a_6 = a_5^2 = (120)^2 = 14400 \equiv 48 \pmod{312}$$
$$c_6 = c_5 = 144 \pmod{312}$$
$$k_6 = \left\lfloor \frac{k_5}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = \lfloor 1 \rfloor = 1$$

Por lo tanto, $126^{85} = a_6 \times c_6 = 48 \times 144 = 6912 \equiv 48 \pmod{312}$

Logaritmos discretos

Logaritmo es sinónimo de *exponente*. Cada vez que tengamos una potencia, desde otro ángulo tendremos un logaritmo. Por ejemplo,

$$2^5 = 32 \Leftrightarrow log_2(32) = 5$$

En Aritmética Modular también tenemos logaritmos, que se definen en el conjunto $\mathbb{Z}_n^* = \{ 1, 2, ..., n-1 \}$ siempre que el número natural *n* sea primo y la base del logaritmo sea "un generador de $\mathbb{Z}_n^*$". Estas condiciones permiten asegurar que el logaritmo quede definido para todo elemento de $\mathbb{Z}_n^*$ (esta afirmación está demostrada en la Referencia [6]). Reciben el nombre de *discretos* porque se definen en un conjunto finito, como lo es $\mathbb{Z}_n^*$.

El uso de la Aritmética Modular introduce una importante complejidad al problema; por esta razón el logaritmo discreto se utiliza en Criptografía.

Su importancia se debe a que la seguridad del Algoritmo de Diffie-Hellman se basa en la dificultad para resolver logaritmos discretos.

Actualmente no se conoce ningún algoritmo, para ser implementado en una computadora clásica, que permita calcular logaritmos discretos de una manera eficiente.

Antes de definirlo matemáticamente, introduciremos las siguientes definiciones:

Definición 2.17: Elemento generador de $\mathbb{Z}_n^*$

Sea $a \in \mathbb{Z}_n^* = \{ 1, 2, ..., n-1 \}$. *Diremos que a es un generador de* $\mathbb{Z}_n^*$ *si verifica que*

$$\mathbb{Z}_n^* = \{ a^0, a^1, ..., a^{n-2} \}$$

Definición 2.18: Logaritmo discreto en $\mathbb{Z}_n^*$

Sea n un número primo y $\mathbb{Z}_n^* = \{ 1, 2, ..., n-1 \}$. *Si* $a \in \mathbb{Z}_n^*$ *es un generador de* $\mathbb{Z}_n^*$, *el logaritmo discreto en base "a" de un número* $x \in \mathbb{Z}_n^*$ *es un número* $y \in \mathbb{Z}_n$ *que verifica*:

$$log_a(x) = y \Leftrightarrow a^y = x \quad (en\ \mathbb{Z}_n)$$

El siguiente Ejemplo ilustrará estos conceptos.

Ejemplo 2.19

Sea $\mathbb{Z}_{13}^{*} = \{\ 1\ ,\ 2\ ,\ ...,\ 11\ ,12\ \}$ con la operación producto en $\mathbb{Z}_{13}^{*}$.

1) Probar que el número *2* es un generador de $\mathbb{Z}_{13}^{*}$.

2) Calcular $log_2(x)\ \forall x \in \mathbb{Z}_{13}^{*}$.

3) Probar que el número *5* no es un generador de $\mathbb{Z}_{13}^{*}$.

4) Verificar que $log_5(x)$ no queda definido $\forall x \in \mathbb{Z}_{13}^{*}$.

Solución

1) En este caso, *n = 13.* Verificaremos que

$$\mathbb{Z}_{13}^{*} = \left\{2^0, 2^1, ..., 2^{10}, 2^{11}\right\}$$

Para ello diseñamos la siguiente tabla:

i	**0**	**1**	**2**	**3**	**4**	**5**
$2^i\ (mod\ 13)$	**1**	**2**	**4**	**8**	**3**	**6**

i	**6**	**7**	**8**	**9**	**10**	**11**
$2^i\ (mod\ 13)$	**12**	**11**	**9**	**5**	**10**	**7**

Por lo tanto, las potencias de *2* generan todos los elementos de $\mathbb{Z}_{13}^{*}$.

2) Como *n = 13* es un número primo y las potencias de *2* generan todos los elementos de $\mathbb{Z}_{13}^{*}$, entonces $log_2(x)$ queda definido $\forall x \in \mathbb{Z}_{13}^{*}$. En las tablas siguientes figuran los valores de dicho logaritmo:

x	**1**	**2**	**3**	**4**	**5**	**6**
$log_2(x)$	**0**	**1**	**4**	**2**	**9**	**5**

x	**7**	**8**	**9**	**10**	**11**	**12**
$log_2(x)$	**11**	**3**	**8**	**10**	**7**	**6**

Por ejemplo,

$log_2(5) = 9$ *pues* $2^9 = 5$ *en* $\mathbb{Z}_{13}^{*}$.

$log_2(12) = 6$ *pues* $2^6 = 12$ *en* $\mathbb{Z}_{13}^{*}$.

3) Verificaremos que *5* no es generador de $\mathbb{Z}_{13}^*$:

i	***0***	***1***	***2***	***3***	***4***
$5^i \pmod{13}$	***1***	***5***	***12***	***8***	***1***

Como $\left\{ 5^i \ / \ i \in \mathbb{Z}_{\geq 0} \right\} = \{ 1, 5, 12, 8 \} \neq \mathbb{Z}_{13}^*$, queda probado que 5 no es generador de $\mathbb{Z}_{13}^*$.

4) Como *5* no es generador de $\mathbb{Z}_{13}^*$, $log_5(x)$ no queda definido $\forall x \in \mathbb{Z}_{13}^*$. Por ejemplo, $log_5(10)$ no existe ya que no existe $y \in \mathbb{Z}_{13}^*$ que verifica que $5^y = 10 \pmod{13}$. Ello se debe a que $10 \notin \left\{ 5^i \ / \ i \in \mathbb{Z}_{\geq 0} \right\} = \{ 1, 5, 12, 8 \}$.

Observación 2.20

Cabe plantearnos lo siguiente: Si *n* es un número primo, ¿existirá algún $a \in \mathbb{Z}_n^*$ que sea generador de $\mathbb{Z}_n^*$? La respuesta es que sí existe, y la prueba de esta afirmación está desarrollada en [6].

El problema de los logaritmos discretos

Nos preguntamos si existe algún algoritmo que permita calcular logaritmos discretos de una manera más sencilla, sin hacerlo *a fuerza bruta*. La respuesta es NO, y mientras más grande sea el módulo *n*, mayor será el tiempo que tome hallar el logaritmo.
La dificultad del cálculo de los logaritmos discretos es lo que da seguridad al algoritmo de Diffie-Hellman.

2. Estructuras Algebraicas

En esta sección definiremos las estructuras algebraicas de Semigrupo, Grupo, Anillo y Cuerpo. Como veremos más adelante que ciertas estructuras algebraicas de Anillo, como la de los cuaterniones, desempeñan un rol importante en el diseño de los algoritmos criptográficos que analizaremos en este trabajo.

Definición 2.21: Semigrupo

Sea G un conjunto no vacío y $*$ una operación binaria definida sobre los elementos de G. El par $(G, *)$ es un semigrupo si y sólo si verifica las siguientes propiedades:

1) $*$ es Ley de Composición Interna: Si $a, b \in G \Rightarrow a * b \in G$.

2) Propiedad asociativa: Si $a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$.

Definición 2.22: Grupo

Sea G un conjunto no vacío y $*$ *una operación binaria definida sobre los elementos de G. El par* $(G,*)$ *es un grupo si y sólo si verifica las siguientes propiedades:*

1) $*$ *es Ley de Composición Interna: Si* $a,b \in G \Rightarrow a*b \in G$.

2) Propiedad asociativa: Si $a,b,c \in G \Rightarrow (a*b)*c = a*(b*c)$.

3) Existencia de elemento neutro o Identidad: $\exists\, e \in G \,/\, a*e = e*a \;\; \forall a \in G$.

4) Existencia de inversos: $\forall a \in G \;\exists\, a^{-1} \in G \,/\, a * a^{-1} = a^{-1} * a = e$.

Definición 2.23: Grupo abeliano o conmutativo

Un grupo $(G,*)$ *es abeliano si verifica la Propiedad Conmutativa:*

Si $a,b \in G \Rightarrow a*b = b*a$.

Definición 2.24: Anillo

Sea A un conjunto no vacío con 2 leyes de composición interna $*$ *y* $\bullet$ *. La terna* $(A,*,\bullet)$ *es un anillo si:*

1) $(A,*)$ *es un grupo abeliano*

2) $(A,\bullet)$ *es un semigrupo*

3) $\bullet$ *es doblemente distributiva con respecto a* $*$ *, es decir:*

$$a \bullet (b*c) = (a \bullet b)*(a \bullet c)$$

$$(b*c) \bullet a = (b \bullet a)*(c \bullet a) \;\; \forall a, b, c \in A$$

Nota:

Si la operación $\bullet$ es conmutativa, se dice que el Anillo es conmutativo. Si existe elemento neutro con respecto a la operación $\bullet$, que lo simbolizaremos por *1*, se dice que $(A,*,\bullet)$ es un anillo con identidad.

Representaremos al anillo $(A,*,\bullet)$ por $(A,+,\cdot)$ y a su elemento neutro con respecto a la operación +, lo denotaremos por *0*.

Definición 2.25: Anillo con divisores de cero

Un anillo $(A,+,\cdot)$ *tiene divisores de cero si existen elementos no nulos que dan producto nulo. Es decir*

$$\exists\, a, b \in A \;\; con \;\; a \neq 0 \;\wedge\; b \neq 0 \;\; tal\; que \; a \cdot b = 0.$$

Definición 2.26: Cuerpo

La terna $(K,+\ ,\ .)$ *es un cuerpo si verifica:*

1) $(K,+)$ *es un grupo abeliano.*

2) $(K-\{0\},+)$ *es un grupo abeliano.*

3) El producto es distributivo respecto de la suma.

Ejemplo 2.27

---

1) El conjunto

$$\mathbb{Q}\left(\sqrt{2}\right)=\left\{a\sqrt{2}\ \ tal\ que\ \ a\in\mathbb{Q}\right\}$$

Es un Semigrupo bajo la operación suma de números reales.

2) Si *n* es un número primo entonces el par $(\mathbb{Z}_n\ ,\ \bullet)$, es un Grupo abeliano, donde $\bullet$ es el producto en $\mathbb{Z}_n$.

3) Si $n\in\mathbb{N}$, la terna $(\mathbb{Z}_n,+,\bullet)$ es un Anillo conmutativo donde $+$ y $\bullet$ son, respectivamente, la suma y producto en $\mathbb{Z}_n$.

4) Sea $M_n(\mathbb{R})$ el conjunto de matrices de orden *n* a coeficientes reales, es decir,

$$M_n(\mathbb{R})=\left\{\ A=\begin{pmatrix} a_{11} & .... & a_{1n} \\ ... & .... & .... \\ a_{n1} & .... & a_{nn} \end{pmatrix}\ tal\ que\ a_{ij}\in\mathbb{R}\ \ \forall i,j=1,2,...,n\ \right\}$$

Entonces la terna $(M_n(\mathbb{R}),+,\bullet)$ es un Anillo no conmutativo donde $+$ y $\bullet$ son, respectivamente, la suma y producto matricial.

5) El anillo $(\mathbb{Z}_4\ ,+\ ,\ \cdot)$ tiene divisores de cero ya que si tomamos $a = b = 2$, se verifica que $a \cdot b = 0\ \ en\ \mathbb{Z}_4$

6) $(\mathbb{Z},+\ ,\ .)$ no es cuerpo, pues los únicos elementos no nulos que admiten inverso son *1* y *-1*.

7) De acuerdo al Corolario *2.13*, la terna $(\mathbb{Z}_p,+\ ,\ .)$ es un cuerpo si *p* es un número primo.

Definición 2.28: Polinomio en una variable

Sea K un subconjunto de $\mathbb{R}$. Un polinomio en la variable x, a coeficientes en K, es una expresión de la forma

$$f(x) = \sum_{i=0}^{n} a_i \; x^i$$

Donde

$n \in \mathbb{Z}_{\geq 0}$, $a_i \in K \quad \forall i = 0, 1, ..., n$

Definición 2.29: El conjunto de polinomios $K[x]$

Si $K \subseteq \mathbb{R}$, el conjunto de polinomios en la variable x, a coeficientes en K, es

$$K[x] = \left\{ f(x) = \sum_{i=0}^{n} a_i \; x^i \;, con \; n \in \mathbb{Z}_{\geq 0} \; \wedge \; a_i \in K \quad \forall i = 0, 1, ..., n \right\}$$

Ejemplo 2.30

$$\mathbb{Z}_{\geq 0}[x] = \left\{ f(x) = \sum_{i=0}^{n} a_i \; x^i \;, con \; n, a_i \in \mathbb{Z}_{\geq 0} \quad \forall i = 0, 1, ..., n \right\}$$

Si $p \in \mathbb{N}$ entonces

$$\mathbb{Z}_p[x] = \left\{ f(x) = \sum_{i=0}^{n} a_i \; x^i \;, con \; n \in \mathbb{Z}_{\geq 0} \; \wedge \; a_i \in \mathbb{Z}_p \quad \forall i = 0, 1, ..., n \right\}$$

Ejemplo 2.31

Sea $f(x) \in \mathbb{Z}_4[x]$ definido por $f(x) = 2x^3 + 4x^4$, con $x \in \mathbb{Z}_7$. Calcular $f(3)$, según las operaciones de suma y producto definidas en $\mathbb{Z}_7$.

Solución

$$f(3) = 2\left(3^3\right) + 4\left(3^4\right) = 2(27) + 4(81) \equiv 2(6) + 4(4) = 12 + 16 = 28 \equiv 0 \pmod 7$$

Por lo tanto

$$f(3) = 0 \quad en \; \mathbb{Z}_7 .$$

La siguiente Proposición es relevante para fundamentar los modelos criptográficos que desarrollaremos.

Proposición 2.32

Sean $(A,+,\bullet)$ *un anillo con identidad,* $f(x), h(x) \in \mathbb{Z}_{\geq 0}[x] \wedge a \in A$.

Entonces

1) $f(a).h(a) = h(a).f(a)$

2) Si $m \in \mathbb{N}$ *entonces*

$$(f(a))^m . (h(a))^m = (h(a))^m . (f(a))^m$$

Demostración

Véase Referencia [7]. ■

Observación 2.33

Si el anillo $(A,+,\bullet)$ no es conmutativo, en general no se verifica que

$$f(a).h(b) = h(b).f(a)$$

Si $a, b \in A$ *con* $a \neq b$.

En el siguiente Ejemplo corroboramos esta afirmación.

Ejemplo 2.34

Sea $(M_2(\mathbb{R}),+,\bullet)$ el anillo no conmutativo de matrices de orden *2* a coeficientes reales. Sean $A = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}$, $f(x) = x + 1$, $h(x) = x^2$. Probar que

$$f(A) . h(B) \neq h(B) . f(A)$$

Solución

$$f(A) = A + 1.I = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$$

$$h(B) = B^2 = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix}$$

$$f(A) . h(B) = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix} . \begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ 12 & 6 \end{pmatrix}$$

$$h(B) . f(A) = \begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 14 & 10 \\ 0 & 0 \end{pmatrix}$$

Por lo tanto

$$f(A) . h(B) \neq h(B) . f(A)$$

3. Los cuaterniones

Uno de los algoritmos criptográficos propuestos por Jorge Kamlofsky y Pedro Hecht, expuesto en la Referencia [3], utiliza cuaterniones. Por esta razón daremos su definición y enunciaremos sus propiedades básicas.

Mientras que los números complejos se definen como una extensión de los números reales, con la incorporación de la unidad imaginaria i tal que $i^2 = -1$, los cuaterniones constituyen una generalización de los números complejos, al agregar las unidades imaginarias j, k de modo tal que $j^2 = k^2 = i.j.k = -1$. Los cuaterniones fueron inventados por William Hamilton en *1843* para poder demostrar la Conjetura de Euler, que afirmaba que todo número natural n puede expresarse como suma de cuatro cuadrados perfectos, es decir,

$$n = a^2 + b^2 + c^2 + d^2 \quad con \ \ a, b, c, d \in \mathbb{Z}$$

Además, fue el primer ejemplo de estructura de anillo sin divisores de cero y no conmutativo. Sus aplicaciones son muy variadas, y van desde la Geometría, ya que son utilizados para rotar figuras en el espacio de una manera más sencilla, hasta aplicaciones físicas dentro del Electromagnetismo y Mecánica Cuántica, entre otras.

Definición 2.35: Cuaternión

Un cuaternión es un número ***q*** *de la forma:*

$$q = a + b\ i + c\ j + d\ k$$

Donde $a, b, c, d \in \mathbb{R}$ *e* i, j, k *son unidades imaginarias que verifican las siguientes igualdades:*

$$i^2 = j^2 = k^2 = i.j.k = -1$$

Dichas unidades imaginarias tienen la Propiedad Asociativa y además conmutan con cualquier constante real.

El conjunto que engloba a todos los cuaterniones se denomina **H**, simbolizado así en honor al matemático irlandés William R. Hamilton (*1805-1865*), y se lo define como:

Definición 2.36: El conjunto H

El conjunto formado por los cuaterniones es

$$H = \{\ q = a + b\ i + c\ j + d\ k\ : a, b, c, d \in \mathbb{R}\ \}$$

Observemos que $\mathbb{C} \subset H$ considerando $c = d = 0$.

La siguiente Proposición muestra los resultados que se obtienen al multiplicar unidades imaginarias:

Proposición 2.37

Sean i, j, k *las unidades imaginarias que verifican* $i^2 = j^2 = k^2 = i.j.k = -1$. *Entonces*

•	i	j	k
i	**- 1**	k	$-j$
j	$-k$	**-1**	i
k	j	$-i$	**-1**

Demostración

Véase Referencia [6]. ■

La tabla que figura en la Proposición anterior es conocida como la Tabla de Cayley y permitirá definir el producto de cuaterniones. Previamente introduciremos la siguiente definición.

Definición 2.38: El conjugado y el módulo de un cuaternión

Sea $q = a + b\,i + c\,j + d\,k$ *un cuaternión. Entonces*

1) El conjugado de q es

$$\bar{q} = a - b\,i - c\,j - d\,k$$

2) El módulo de q es

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Si un cuaternión tiene módulo 1 se dice que es un cuaternión unitario.

Operaciones entre cuaterniones

Si $q_1 = a_1 + b_1\,i + c_1\,j + d_1\,k$ y $q_2 = a_2 + b_2\,i + c_2\,j + d_2\,k$ son dos cuaterniones entonces:

Suma de cuaterniones

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2)\,i + (c_1 + c_2)\,j + (d_1 + d_2)\,k$$

Producto de cuaterniones

El producto se lo define teniendo en cuenta la Tabla de Cayley y aplicando la propiedad distributiva del producto con respecto a la suma:

$$q_1.q_2 = (a_1 + b_1\,i + c_1\,j + d_1\,k).(a_2 + b_2\,i + c_2\,j + d_2\,k) =$$

$$= a_1\ a_2 + a_1\ b_2\ i + a_1\ c_2\ j + a_1\ d_2\ k + b_1\ a_2\ i + b_1\ b_2\ i^2 + b_1\ c_2\ i\,j +$$
$$+ b_1\ d_2\ i\,k + c_1\ a_2\ j + c_1\ b_2\ j\ i + c_1\ c_2\ j\,j + c_1\ d_2\ j\,k + d_1\ a_2\ k + d_1\ b_2\ k\,i +$$
$$+ d_1\ c_2\ k\,j + d_1\ d_2\ k\,k =$$
$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2\ )i +$$
$$+ (a_1c_2 + a_2c_1 + d_1b_2 - b_1d_2\ )j + (a_1d_2 + b_1c_2 + d_1a_2 - c_1b_2\ )k$$

Con estas definiciones de suma y producto, la terna $(H, +, \bullet)$ forma un anillo no conmutativo.

El módulo de un cuaternión expresado en términos de su conjugado

De acuerdo a la definición de producto de cuaterniones, se puede comprobar que

$$|\ q\ | = \sqrt{q.\ \bar{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Cociente de cuaterniones

Si $q_2 \neq 0$ entonces:

$$\frac{q_1}{q_2} = \frac{q_1.\ \overline{q_2}}{q_2.\ \overline{q_2}} = \frac{q_1.\ \overline{q_2}}{|\ q_2\ |^2}$$

Inverso de un cuaternión

Dado un cuaternión $q \neq 0$, su inverso es $q^{-1} = \frac{1}{q} = \frac{\bar{q}}{q.\ \bar{q}} = \frac{\bar{q}}{|\ q\ |^2}$

Normalización de un cuaternión

Dado un cuaternión $q \neq 0$ cuyo módulo no sea igual a uno, se lo puede normalizar definiendo un nuevo cuaternión unitario, asociado al primero, mediante la operación:

$$q_1 = \frac{q}{|\ q\ |}$$

Diferentes representaciones de un cuaternión

Existen diversas maneras de expresar un cuaternión. Según cómo se quiera operar con él, es conveniente expresarlo de una determinada forma. Dado un cuaternión ***q***, sus distintas representaciones son:

***Forma vectorial*:**

Es la forma en la que se definió el cuaternión. Es decir,

$$q = a + b\ i + c\ j + d\ k$$

***Forma cartesiana*:**

Consiste en representar al cuaternión como un vector en $\mathbb{R}^4$, es decir,

$$q = (a,\ b\ ,\ c\ ,\ d\ )$$

***Forma trigonométrica*:**

Es muy utilizada para calcular las potencias de un cuaternión. El siguiente teorema justifica esta representación.

Teorema 2.39: Forma trigonométrica de un cuaternión

Sea $q = a + b\,i + c\,j + d\,k$ *con* $q \neq 0$ *. Entonces*

$$q = |q| \left(\cos(\theta) + sen(\theta)\ .\ v'\right)$$

Donde

$$\theta = \arccos\left(\frac{a}{|q|}\right) \quad , 0 \leq \theta \leq \pi$$

$$v' = \begin{cases} 0 & si\ b = c = d = 0 \\ \dfrac{b\,i + c\,j + d\,k}{|b\,i + c\,j + d\,k|} & en\ otro\ caso \end{cases}$$

O expresado en forma cartesiana,

$$v' = \begin{cases} 0 & si\ b = c = d = 0 \\ \dfrac{(b\ ,c\ ,d)}{|(b\ ,c\ ,d)|} & en\ otro\ caso \end{cases}$$

Demostración

Véase Referencia [6]. ■

El siguiente ejemplo ilustra cómo expresar en forma trigonométrica un cuaternión escrito en forma vectorial.

Ejemplo 2.40

Expresar en forma trigonométrica el cuaternión $q = 3 + i + 3\,j + \sqrt{6}\ k$

Solución

En este caso, $a = 3$, $b = 1$, $c = 3$, $d = \sqrt{6}$. Entonces

$$|q| = \sqrt{3^2 + 1^2 + 3^2 + \left(\sqrt{6}\right)^2} = \sqrt{25} = 5$$

Operando con dos decimales, tenemos

$$\theta = \arccos\left(\frac{a}{|q|}\right) = \arccos\left(\frac{3}{5}\right) = 0.92$$

$$v' = \frac{b\,i + c\,j + d\,k}{|b\,i + c\,j + d\,k|} = \frac{i + 3\,j + \sqrt{6}\ k}{\sqrt{1^2 + 3^2 + \left(\sqrt{6}\right)^2}} = \frac{i + 3\,j + \sqrt{6}\ k}{4}$$

O expresado en forma cartesiana:

$$v' = \frac{\left(1,\ 3,\ \sqrt{6}\right)}{4}$$

Por lo tanto,

$$q = |\ q\ |\ \left(cos\left(\theta\right) + sen\left(\theta\right).\ v'\right) = 5\ \left(cos\left(0.92\right) + sen\left(0.92\right)\ .\ \frac{\left(1,\ 3,\ \sqrt{6}\right)}{4}\right)$$

Potencia de un cuaternión

La forma trigonométrica de un cuaternión permitirá calcular, de una manera más sencilla, la potencia de exponente natural de un cuaternión.

Teorema 2.41: Fórmula de De Moivre para cuaterniones

Sea $q = a + b\ i + c\ j + d\ k$ *un cuaternión o nulo cuya forma trigonométrica es*

$$q = |\ q\ |\ \left(cos\left(\theta\right) + sen\left(\theta\right)\ .\ v'\right)\ .$$

Si $n \in \mathbb{N}$ *entonces*

$$q^n = |\ q\ |^n\ \left(cos\left(n\ \theta\right) + sen\left(n\ \theta\right)\ .\ v'\right)$$

Demostración

Véase Referencia [6]. ■

Ejemplo 2.42

Si $q = 3 + i + 3\ j + \sqrt{6}\ k$, calcular q^{100}.

Solución

Del Ejemplo *2.40*, sabemos que

$$q = |\ q\ |\ \left(cos\left(\theta\right) + sen\left(\theta\right).\ v'\right) = 5\ \left(cos\left(0.92\right) + sen\left(0.92\right)\ .\ \frac{\left(1,\ 3,\ \sqrt{6}\right)}{4}\right)$$

Luego, por la Fórmula de De Moivre aplicada a cuaterniones, resulta

$$q^{100} = 5^{100}\ \left(cos\left(100 \times 0.92\right) + sen\left(100 \times 0.92\right)\ .\ \frac{\left(1,\ 3,\ \sqrt{6}\right)}{4}\right) =$$

$$= 5^{100}\ \left(cos\left(92\right) + sen\left(92\right)\ .\ \frac{\left(1,\ 3,\ \sqrt{6}\right)}{4}\right).$$

Si bien el anillo de los cuaterniones no es conmutativo ya que, por ejemplo, $i\,.\,j \neq j\,.\,i$, bajo ciertas condiciones algunos cuaterniones sí conmutan. La siguiente Proposición muestra algunos casos en los cuales esta propiedad se verifica.

Proposición 2.43:

Si q *es un cuaternión,* $a \in \mathbb{R}$ *y* $m,n \in \mathbb{N}$ *entonces*

1) $a \,.\, q = q \,.\, a$

2) Si $f(x) = \sum_{i=0}^{n} a_i . x^i$, $h(x) = \sum_{i=0}^{n} b_i . x^i$ *con* $a_i, b_i \in \mathbb{R}$ $\forall$ *i=1,...,n entonces*

a) $f(q) \,.\, h(q) = h(q) \,.\, f(q)$

b) $[f(q)]^m . [h(q)]^m = [h(q)]^m . [f(q)]^m$

Demostración

1) Sea el cuaternión $q = a_1 + a_2\, i + a_3\, j + a_4\, k$. Entonces, aplicando la Propiedad Conmutativa del producto de números reales, obtenemos

$$a \,.\, q = a.(a_1 + a_2\, i + a_3\, j + a_4\, k) = a.a_1 + a.a_2\, i + a.a_3\, j + a.a_4\, k =$$

$$= a_1.a + a_2.a\, i + a_3.a\, j + a_4.a\, k = (a_1 + a_2\, i + a_3\, j + a_4\, k) . a = q . a$$

2)

a) Resulta de aplicar la Proposición *2.31* inciso *1*).

b) Resulta de aplicar la Proposición *2.31* inciso 2). ■

Ejemplo 2.44

Si $q = 1 + \sqrt{3}\, k$ y $f(x) = x^3 + 10$,calcular $[f(q)]^5$.

Solución

Primeramente expresamos *q* en forma trigonométrica:

$$q = 2 \left(cos\left(\frac{\pi}{3}\right) + sen\left(\frac{\pi}{3}\right) . (0,\, 0,\, 1) \right)$$

Entonces, aplicando la Fórmula de De Moivre resulta

$$f(q) = q^3 + 10 = 2^3 \left(cos\left(3 \times \frac{\pi}{3}\right) + sen\left(3 \times \frac{\pi}{3}\right) . (0,\, 0,\, 1) \right) + 10 =$$

$$= 8 \left(cos(\pi) + sen(\pi) . (0,\, 0,\, 1) \right) + 10 = 8\, (-1 + 0) + 10 = -8 + 10 = 2$$

Por lo tanto

$$[f(q)]^5 = 2^5 = 32$$

Existe un conjunto más amplio que el de los cuaterniones, llamado el *conjunto de los octoniones*. Este tipo de estructura se aplica en el Protocolo HK17, que veremos en el Capítulo *4*. En la próxima sección profundizaremos en este conjunto.

4. Los octoniones

Los octoniones surgieron como una extensión no asociativa de los cuaterniones. Fueron inventados por John T. Graves en *1843* e independientemente por Arthur Cayley, quien lo publicó por primera vez en *1845*. Por esta razón son a veces llamados *Los números de Cayley*. Su definición es la siguiente:

Definición 2.45: Octonión

Un octonión ***o*** *es una expresión de la forma*

$$o = \sum_{i=0}^{7} a_i \ e_i$$

Donde $a_i \in \mathbb{R} \ \forall \ i = 0, 1, ..., 7$

$e_1, e_2, \ldots, e_7$ *son unidades imaginarias y* $e_0 = 1$.

El conjunto de todos los octoniones se denomina **O**. Observemos que los cuaterniones forman un subconjunto de los octoniones, es decir

$$H \subset O$$

Considerando $e_0 = 1$, $e_1 = i$, $e_2 = j$, $e_4 = k$, $a_3 = a_5 = a_6 = a_7 = 0$.

Al principio, los octoniones no parecieron ofrecer aplicaciones a la Geometría ni a la Física, como ocurre con los cuaterniones. Sin embargo, en la década de los ochenta, el concepto de los octoniones se utilizó para dar un marco teórico a una de las teorías más nuevas de la Física: *La Teoría de Cuerdas*.

Esta Teoría describe de qué manera actúan las fuerzas y todo tipo de materia existente en el Universo, desde un átomo hasta un planeta. De este modo unifica, bajo las mismas leyes, la Física Cuántica con la Física Newtoniana. La Teoría establece que las partículas más elementales del universo no son objetos puntuales, sino que tienen forma de cuerda y que vibran del mismo modo que lo hacen las cuerdas de un instrumento musical. Definiremos a continuación algunos conceptos que precisaremos para trabajar con los octoniones.

Definición 2.46: El conjugado y el módulo de un octonión

Sea $o = \sum_{i=0}^{7} a_i \ e_i$ *un octonión. Entonces*

1) El conjugado de o *es*

$$\bar{o} = a_0 - \sum_{i=1}^{7} a_i \ e_i$$

2) El módulo de o *es*

$$| o | = \sqrt{\sum_{i=0}^{7} a_i^2}$$

Operaciones entre octoniones

Si $o_1 = \sum_{i=0}^{7} a_i \ e_i$ y $o_2 = \sum_{i=0}^{7} b_i \ e_i$ son dos octoniones entonces:

Suma de octoniones

$$o_1 + o_2 = \sum_{i=0}^{7} a_i \ e_i + \sum_{i=0}^{7} b_i \ e_i = \sum_{i=0}^{7} (a_i + b_i \ ) e_i$$

Producto de octoniones

El producto se lo define teniendo en cuenta la siguiente Tabla, que indica cómo se multiplican las unidades imaginarias:

$\cdot$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	e_2	$-e_4$	-1	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	e_3	$-e_7$	$-e_5$	-1	e_6	e_2	$-e_4$	e_1
e_4	e_4	e_2	$-e_1$	$-e_6$	-1	e_7	e_3	$-e_5$
e_5	e_5	$-e_6$	e_3	$-e_2$	$-e_7$	-1	e_1	e_4
e_6	e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	-1	e_2
e_7	e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	-1

Tabla 2.1: Tabla producto entre unidades imaginarias.

De este modo, para multiplicar dos octoniones se utiliza la Tabla anterior y se aplica la propiedad distributiva del producto con respecto a la suma. Así, obtenemos:

$$o_1 \cdot o_2 = \left(\sum_{i=0}^{7} a_i \ e_i \right) \cdot \left(\sum_{i=0}^{7} b_i \ e_i \right) =$$

$$(a_0 \ b_0 - a_1 \ b_1 - a_2 \ b_2 - a_3 \ b_3 - a_4 \ b_4 - a_5 \ b_5 - a_6 \ b_6 - a_7 \ b_7). e_0 +$$

$$(a_0 \ b_1 + a_1 \ b_0 + a_2 \ b_4 + a_3 \ b_7 - a_4 \ b_2 + a_5 \ b_6 - a_6 \ b_5 - a_7 \ b_3). e_1 +$$

$$(a_0 \ b_2 - a_1 \ b_4 + a_2 \ b_0 + a_3 \ b_5 + a_4 \ b_1 - a_5 \ b_3 + a_6 \ b_7 - a_7 \ b_6). e_2 +$$

$$(a_0 \ b_3 - a_1 \ b_7 - a_2 \ b_5 + a_3 \ b_0 + a_4 \ b_6 + a_5 \ b_2 - a_6 \ b_4 + a_7 \ b_1). e_3 +$$

$$(a_0 \ b_4 + a_1 \ b_2 - a_2 \ b_1 - a_3 \ b_6 + a_4 \ b_0 + a_5 \ b_7 + a_6 \ b_3 - a_7 \ b_5). e_4 +$$

$$(a_0 \ b_5 - a_1 \ b_6 + a_2 \ b_3 - a_3 \ b_2 - a_4 \ b_7 + a_5 \ b_0 + a_6 \ b_1 + a_7 \ b_4). e_5 +$$

$$(a_0 \ b_6 + a_1 \ b_5 - a_2 \ b_7 + a_3 \ b_4 - a_4 \ b_3 - a_5 \ b_1 + a_6 \ b_0 + a_7 \ b_2). e_6 +$$

$$(a_0 \ b_7 + a_1 \ b_3 + a_2 \ b_6 - a_3 \ b_1 + a_4 \ b_5 - a_5 \ b_4 - a_6 \ b_2 + a_7 \ b_0). e_7 +$$

En base a esta definición de producto, podemos comprobar que si $o = \sum_{i=0}^{7} a_i \ e_i$ y $a \in \mathbb{R}$ entonces $o.\ a = a.\ o$. Sin embargo, el producto de octoniones no siempre goza de la propiedad conmutativa ni de la asociativa. Por ejemplo,

$$e_1 . e_2 = e_4$$

Mientras que

$$e_2 . e_1 = - e_4$$

Luego,

$$e_1 . e_2 \neq e_2 . e_1$$

Por otro lado,

$$(e_1 . e_2). e_3 = e_4 . e_3 = - e_6$$

Mientras que

$$e_1 . (e_2 . e_3) = e_1 . e_5 = e_6 .$$

Por lo tanto

$$(e_1 . e_2). e_3 \neq e_1 . (e_2 . e_3)$$

Con estas definiciones de suma y producto, la terna $(O,+, \cdot)$ no es un anillo ya que $(O, \cdot)$ no es un semigrupo.

Cociente de octoniones

Sean o_1 , o_2 dos octoniones con $o_2 \neq 0$. Entonces:

$$\frac{o_1}{o_2} = \frac{o_1 . \overline{o_2}}{o_2 . \overline{o_2}} = \frac{o_1 . \overline{o_2}}{|\ o_2\ |^2}$$

Inverso de un octonión

Si o un octonión con $o \neq 0$, su inverso es

$$o^{-1} = \frac{1}{o} = \frac{\bar{o}}{o\ .\ \bar{o}} = \frac{\bar{o}}{|\ o\ |^2}$$

El módulo de un octonión expresado en términos de su conjugado

De acuerdo a la definición de producto de octoniones, se puede comprobar que si o es un octonión entonces

$$|\ o\ | = \sqrt{o.\ \bar{o}} = \sqrt{\sum_{i=0}^{7} a_i^2}$$

La siguiente Proposición prueba una propiedad que tienen los octoniones con parte real nula.

Proposición 2.47:

Sea ***o*** *un octonión tal que*

$$o = \sum_{i=1}^{7} a_i \ e_i$$

Entonces

$$o^2 = -\sum_{i=1}^{7} a_i^2$$

Demostración

Aplicando la definición de producto entre dos octoniones, tenemos que:

$$o^2 = o \ . \ o = \left(\sum_{i=1}^{7} a_i \ e_i \right) \cdot \left(\sum_{i=1}^{7} a_i \ e_i \right) = \left(-\sum_{i=1}^{7} a_i^2 \right) e_0 = \left(-\sum_{i=1}^{7} a_i^2 \right) .1 = -\sum_{i=1}^{7} a_i^2 . \ \blacksquare$$

Diferentes representaciones de un octonión

Al igual que los cuaterniones, existen diversas maneras de expresar un octonión, según cómo se quiera operar con él. Dado un cuaternión ***o***, sus distintas representaciones son:

***Forma vectorial*:**

Es la forma en la que se definió el octonión. Es decir,

$$o = \sum_{i=0}^{7} a_i \ e_i$$

***Forma cartesiana*:**

Consiste en representar al octonión como un vector en $\mathbb{R}^8$, es decir,

$$o = (a_0 , a_1 , a_2 , a_3 , a_4 , a_5 , a_6 , a_7) \ \ con \ a_i \in \mathbb{R} \ \forall \ i = 0 , 1 , \dots , 7.$$

***Forma trigonométrica*:**

Tal como ocurre con los cuaterniones, la forma trigonométrica es utilizada para calcular las potencias de un octonión. El siguiente teorema muestra cómo es esta representación.

Teorema 2.48: Forma trigonométrica de un octonión

Sea $o = \sum_{i=0}^{7} a_i \ e_i$ *un octonión no nulo. Entonces*

$$o = |\, o \,| \left(cos\left(\theta\right) + sen\left(\theta\right) \,.\, \nu\,' \right)$$

Donde

$$\theta = ar\cos\left(\frac{a_0}{|\, o \,|} \right), \ 0 \le \theta \le \pi$$

$$\nu\,' = \begin{cases} 0 & si \ a_i = 0 \ \ \forall \ i = 1, 2, ..., 7 \\ \dfrac{\sum_{i=1}^{7} a_i \ e_i}{\left| \sum_{i=1}^{7} a_i \ e_i \right|} & en\ otro\ caso \end{cases}$$

Demostración

1) Si $a_i \neq 0$ para algún $i = 1, 2..., 7$ entonces

$$o = |\, o \,| \left(\frac{a_0}{|\, o \,|} + \frac{\sum_{i=1}^{7} a_i \ e_i}{|\, o \,|} \cdot \frac{\left| \sum_{i=1}^{7} a_i \ e_i \right|}{\left| \sum_{i=1}^{7} a_i \ e_i \right|} \right) \qquad [1]$$

Si definimos

$$\nu = \sum_{i=1}^{7} a_i \ e_i$$

$$\nu\,' = \frac{\sum_{i=1}^{7} a_i \ e_i}{\left| \sum_{i=1}^{7} a_i \ e_i \right|}$$

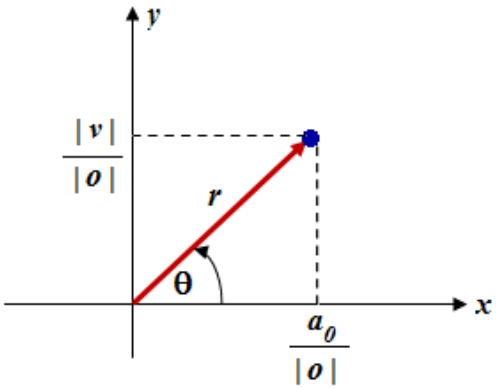
Y se reemplaza estas expresiones en [1] resulta:

$$o = |\, o \,| \left(\frac{a_0}{|\, o \,|} + \frac{|\, \nu \,|}{|\, o \,|} \cdot \nu\,' \right) \qquad [2]$$

Si se considera el siguiente punto del plano:

$$o = \left(\frac{a_0}{|\, o \,|} \ , \ \frac{|\, \nu \,|}{|\, o \,|} \right)$$

Entonces dicho punto se encuentra en el primer o segundo cuadrante, según sea $a_0 \geq 0$ o bien $a_0 < 0$. Si se lo expresa en coordenadas polares, tenemos:



Por lo tanto

$$\begin{cases} cos(\theta) = \dfrac{\dfrac{a_0}{|o|}}{r} \\ sen(\theta) = \dfrac{\dfrac{|v|}{|o|}}{r} \end{cases} \Rightarrow \begin{cases} \dfrac{a_0}{|o|} = r.cos(\theta) \\ \dfrac{|v|}{|o|} = r.sen(\theta) \end{cases}$$

Como $\dfrac{|v|}{|o|} \geq 0$, obtenemos que $0 \leq \theta \leq \pi$. Por otro lado, como

$$\left(\frac{a_0}{|o|}\right)^2 + \left(\frac{|v|}{|o|}\right)^2 = \left(r.cos(\theta)\right)^2 + \left(r.sen(\theta)\right)^2 = r^2$$

Y además

$$\left(\frac{a_0}{|o|}\right)^2 + \left(\frac{|v|}{|o|}\right)^2 = \frac{a_0^2 + |v|^2}{|o|^2} = \frac{a_0^2 + \sum_{i=1}^{7} a_i^2}{|o|^2} = \frac{\sum_{i=0}^{7} a_i^2}{|o|^2} = \frac{|o|^2}{|o|^2} = 1$$

Entonces $r^2 = 1$ y por lo tanto $r = 1$. Así,

$$\begin{cases} \dfrac{a_0}{|o|} = cos(\theta) \\ \dfrac{|v|}{|o|} = sen(\theta) \end{cases} \qquad [3]$$

Reemplazando [3] en [2] tenemos:

$$o = |o| \left(cos(\theta) + sen(\theta) \cdot v'\right)$$

Donde

$$\theta = ar\,cos\left(\frac{a_0}{|o|}\right) \;,\; 0 \leq \theta \leq \pi$$

2) Si $a_i = 0 \;\; \forall \; i = 1, 2, ..., 7$ entonces $o = a_0$. Por otro lado,

$$cos\left(\theta\right)=\frac{a_0}{\left|\,o\,\right|}=\frac{a_0}{\left|\,a_0\,\right|}$$

Luego, teniendo en cuenta que $v' = 0$ obtenemos

$$o=a_0=\left|a_0\right|\ \frac{a_0}{\left|a_0\right|}=\left|a_0\right|\ cos\left(\theta\right)=\left|\,o\,\right|\ cos\left(\theta\right)=\left|\,o\,\right|\ \left(cos\left(\theta\right)+sen\left(\theta\right).\,v'\right)\quad\blacksquare$$

El siguiente ejemplo mostraremos cómo expresar en forma trigonométrica un octonión escrito en forma vectorial.

Ejemplo 2.49

Expresar en forma trigonométrica el octonión

$$o=1+\frac{1}{2}\ e_1+\sqrt{2}\ e_2+\frac{1}{4}\ e_3+\frac{1}{2}\ e_6+\frac{\sqrt{7}}{4}\ e_7$$

Solución

En este caso,

$$a_0=1,\ a_1=\frac{1}{2}\ ,\ a_2=\sqrt{2}\ ,a_3=\frac{1}{4}\ ,a_4=0,\ a_5=0\ ,a_6=\frac{1}{2},\ a_7=\frac{\sqrt{7}}{4}.$$

Entonces

$$\left|\,o\,\right|=\sqrt{1^2+\left(\frac{1}{2}\right)^2+\left(\sqrt{2}\right)^2+\left(\frac{1}{4}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{\sqrt{7}}{4}\right)^2}=2$$

$$\theta=ar\,cos\left(\frac{a_0}{\left|\,o\,\right|}\right)=ar\,cos\left(\frac{1}{2}\right)=\frac{\pi}{3}$$

$$v'=\frac{\sum_{i=1}^{7}a_i\ e_i}{\left|\sum_{i=1}^{7}a_i\ e_i\right|}=\frac{\frac{1}{2}\ e_1+\sqrt{2}\ e_2+\frac{1}{4}\ e_3+\frac{1}{2}\ e_6+\frac{\sqrt{7}}{4}\ e_7}{\sqrt{\left(\frac{1}{2}\right)^2+\left(\sqrt{2}\right)^2+\left(\frac{1}{4}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{\sqrt{7}}{4}\right)^2}}=$$

$$=\frac{\frac{1}{2}\ e_1+\sqrt{2}\ e_2+\frac{1}{4}\ e_3+\frac{1}{2}\ e_6+\frac{\sqrt{7}}{4}\ e_7}{\sqrt{3}}=$$

$$=\frac{1}{2\sqrt{3}}\ e_1+\frac{\sqrt{2}}{\sqrt{3}}\ e_2+\frac{1}{4\sqrt{3}}\ e_3+\frac{1}{2\sqrt{3}}\ e_6+\frac{\sqrt{7}}{4\sqrt{3}}\ e_7$$

O expresado en forma cartesiana:

$$v'=\left(\frac{1}{2\sqrt{3}}\ ,\frac{\sqrt{2}}{\sqrt{3}}\ ,\frac{1}{4\sqrt{3}}\ ,0\ ,0\ ,\frac{1}{2\sqrt{3}},\frac{\sqrt{7}}{4\sqrt{3}}\right)$$

Por lo tanto,

$$o = |\, o \,| \left(\cos(\theta) + sen(\theta)\ .\ v'\right) = 2\ \left(\cos\left(\frac{\pi}{3}\right) + sen\left(\frac{\pi}{3}\right)\ .\ v'\right) =$$

$$= 2\ \left(\cos\left(\frac{\pi}{3}\right) + sen\left(\frac{\pi}{3}\right)\ .\ \left(\frac{1}{2\sqrt{3}}\ e_1 + \frac{\sqrt{2}}{\sqrt{3}}\ e_2 + \frac{1}{4\sqrt{3}}\ e_3 + \frac{1}{2\sqrt{3}}\ e_6 + \frac{\sqrt{7}}{4\sqrt{3}}\ e_7\right)\right)$$

O bien

$$o = 2\ \left(\cos\left(\frac{\pi}{3}\right) + sen\left(\frac{\pi}{3}\right)\ .\ \left(\frac{1}{2\sqrt{3}}\ , \frac{\sqrt{2}}{\sqrt{3}}\ , \frac{1}{4\sqrt{3}}\ , 0\ , 0\ ,\ \frac{1}{2\sqrt{3}}, \frac{\sqrt{7}}{4\sqrt{3}}\right)\right)$$

Cálculo de potencias de un octonión

Tal como sucede con los cuaterniones, la forma trigonométrica de un octonión permitirá calcular, mediante la Fórmula de De Moivre, la potencia de exponente natural de un octonión. El siguiente Teorema enuncia esta fórmula.

Teorema 2.50: Fórmula de De Moivre para octoniones

Sea $o = \sum_{i=0}^{7} a_i\ e_i$ *un octonión no nulo cuya fórmula trigonométrica es*

$$o = |\, o \,| \left(\cos(\theta) + sen(\theta)\ .\ v'\right)$$

Si $n \in \mathbb{N}$ *entonces*

$$o^n = |\, o \,|^n\ \left(\cos(n\ \theta) + sen(n\ \theta)\ .\ v'\right)$$

Demostración

Aplicaremos el Principio de Inducción sobre *n*.
Para *n = 1* se verifica claramente pues

$$o^1 = o = |\, o \,| \left(\cos(\theta) + sen(\theta)\ .\ v'\right) = |\, o \,|^1\ \left(\cos(1.\ \theta) + sen(1.\ \theta)\ .\ v'\right)$$

Suponemos ahora que la igualdad es válida para *n* (Hipótesis Inductiva). Es decir,

$$o^n = |\, o \,|^n\ \left(\cos(n\ \theta) + sen(n\ \theta)\ .\ v'\right)$$

Con

$$v' = \begin{cases} 0 & si\ \ a_i = 0\ \ \forall\ i = 1, 2, ..., 7 \\ \dfrac{\sum_{i=1}^{7} a_i\ e_i}{\left|\sum_{i=1}^{7} a_i\ e_i\right|} & en\ otro\ caso \end{cases}$$

Demostraremos que la igualdad es válida para (*n+1*):

1) Si $a_i \neq 0$ para algún $i = 1, 2..., 7$, entonces por la Proposición *2.50* tenemos que $(\nu')^2 = -1$ pues

$$(\nu')^2 = \frac{\sum_{i=1}^{7} a_i\ e_i}{\left|\sum_{i=1}^{7} a_i\ e_i\right|} \cdot \frac{\sum_{i=1}^{7} a_i\ e_i}{\left|\sum_{i=1}^{7} a_i\ e_i\right|} = \frac{\left(\sum_{i=1}^{7} a_i\ e_i\right)^2}{\left|\sum_{i=1}^{7} a_i\ e_i\right|^2} = \frac{-\sum_{i=1}^{7} a_i^2}{\sum_{i=1}^{7} a_i^2} = -1$$

Por lo tanto, haciendo uso de la Hipótesis Inductiva resulta

$$o^{n+1} = o^n . o = \underbrace{|o|^n \left(\cos(n\theta) + sen(n\theta) . \nu'\right)}_{Hipótesis\ Inductiva} . |o| \left(\cos(\theta) + sen(\theta) . \nu'\right) =$$

$$= |o|^n . |o| \left(\cos(n\theta) + sen(n\theta) . \nu'\right).\left(\cos(\theta) + sen(\theta) . \nu'\right) =$$

$$= |o|^{n+1} \left(\cos(n\theta) + sen(n\theta) . \nu'\right).\left(\cos(\theta) + sen(\theta) . \nu'\right) =$$

$$= |o|^{n+1} \left(\cos(n\theta).\cos(\theta) + \cos(n\theta).sen(\theta).\nu' + sen(n\theta).\nu'.\cos(\theta) + sen(n\theta).\nu'.sen(\theta).\nu'\right) =$$

$$= |o|^{n+1} \left(\cos(n\theta).\cos(\theta) + \cos(n\theta).sen(\theta).\nu' + sen(n\theta).\cos(\theta).\nu' + sen(n\theta).sen(\theta).(\nu')^2\right) =$$

$$= |o|^{n+1} \left(\cos(n\theta).\cos(\theta) + \cos(n\theta).sen(\theta).\nu' + sen(n\theta).\cos(\theta).\nu' - sen(n\theta).sen(\theta)\right) =$$

$$= |o|^{n+1} \left(\cos(n\theta).\cos(\theta) - sen(n\theta).sen(\theta) + \left(\cos(n\theta).sen(\theta) + sen(n\theta).\cos(\theta)\right).\nu'\right) =$$

$$= |o|^{n+1} \left(\cos(n\theta + \theta) + sen(n\theta + \theta).\nu'\right) = |o|^{n+1} \left(\cos((n+1)\theta) + sen((n+1)\theta).\nu'\right)$$

2) Si $a_i = 0\ \forall\ i = 1, 2, ..., 7$, la demostración es trivial. ■

Ejemplo 2.51

Dado el octonión

$$o = 1 + \frac{1}{2}\ e_1 + \sqrt{2}\ e_2 + \frac{1}{4}\ e_3 + \frac{1}{2}\ e_6 + \frac{\sqrt{7}}{4}\ e_7$$

Calcular o^{12}.

Solución

En el Ejemplo *2.49*, vimos que la expresión trigonométrica de o es:

$$o = 2\left(\cos\left(\frac{\pi}{3}\right)+sen\left(\frac{\pi}{3}\right).\left(\frac{1}{2\sqrt{3}},\frac{\sqrt{2}}{\sqrt{3}},\frac{1}{4\sqrt{3}},0,0,\frac{1}{2\sqrt{3}},\frac{\sqrt{7}}{4\sqrt{3}}\right)\right)$$

Por lo tanto, aplicando la Fórmula de De Moivre, resulta

$$o^{12} = 2^{12}\left(\cos\left(12.\frac{\pi}{3}\right)+sen\left(12.\frac{\pi}{3}\right).\left(\frac{1}{2\sqrt{3}},\frac{\sqrt{2}}{\sqrt{3}},\frac{1}{4\sqrt{3}},0,0,\frac{1}{2\sqrt{3}},\frac{\sqrt{7}}{4\sqrt{3}}\right)\right)=$$

$$= 2^{12}\left(\cos(4\pi)+sen(4\pi).\left(\frac{1}{2\sqrt{3}},\frac{\sqrt{2}}{\sqrt{3}},\frac{1}{4\sqrt{3}},0,0,\frac{1}{2\sqrt{3}},\frac{\sqrt{7}}{4\sqrt{3}}\right)\right)=$$

$$= 2^{12}\left(1+0.\left(\frac{1}{2\sqrt{3}},\frac{\sqrt{2}}{\sqrt{3}},\frac{1}{4\sqrt{3}},0,0,\frac{1}{2\sqrt{3}},\frac{\sqrt{7}}{4\sqrt{3}}\right)\right)=2^{12}=4096.$$

Como mencionamos anteriormente, el producto de octoniones no siempre satisface la Propiedad Asociativa y la Conmutativa.
Las siguientes Proposiciones muestran algunos casos en los cuales se verifican estas Propiedades.

Proposición 2.52

Sea $o=\sum_{i=0}^{7} a_i\ e_i$ *un octonión,* $a,b\in\mathbb{R}$ *y* $m,n\in\mathbb{N}$. *Entonces*

1) $a.o=o.a$

2) $o^m.o^n=o^{m+n}$

3) Si o_1 , o_2 *son dos octoniones entonces*

$$(a.o_1).(b.o_2)=(a.b).(o_1.o_2)$$

Demostración

1) De la definición de producto entre dos octoniones y aplicando la Propiedad Conmutativa del producto de números reales, resulta

$$a.o=a.\sum_{i=0}^{7} a_i\ e_i=\sum_{i=0}^{7}(a.a_i)\ e_i=\sum_{i=0}^{7}(a_i.a)\ e_i$$

Por otro lado,

$$o.a=\left(\sum_{i=0}^{7} a_i\ e_i\right).a=\sum_{i=0}^{7}(a_i.a)\ e_i$$

Luego,

$$a.o=o.a$$

2) Consideremos la representación trigonométrica de o . Es decir,

$$o = |\, o \,| \left(\cos(\theta) + sen(\theta)\ .\ \nu'\right)$$

Entonces, por la Fórmula de De Moivre (Teorema *2.50*) tenemos:

$$o^m = |\, o \,|^m \ \left(\cos(m\,\theta) + sen(m\,\theta)\ .\ \nu'\right)$$

$$o^n = |\, o \,|^n \ \left(\cos(n\ \theta) + sen(n\ \theta)\ .\ \nu'\right)$$

Por lo tanto, teniendo en cuenta que $(\nu')^2 = -1$ resulta:

$$o^m . o^n = |\, o \,|^m \ \left(\cos(m\,\theta) + sen(m\,\theta)\ .\ \nu'\right). \ |\, o \,|^n \ \left(\cos(n\,\theta) + sen(n\,\theta)\ .\ \nu'\right) =$$

$$= |\, o \,|^m . |\, o \,|^n \ \left(\cos(m\,\theta) + sen(m\,\theta)\ .\ \nu'\right). \left(\cos(n\,\theta) + sen(n\,\theta)\ .\ \nu'\right) =$$

$$= |\, o \,|^{m+n} . \left(\cos(m\,\theta) + sen(m\,\theta)\ .\ \nu'\right). \left(\cos(n\,\theta) + sen(n\,\theta)\ .\ \nu'\right) =$$

$$= |\, o \,|^{m+n} . \left(\cos(m\,\theta).\cos(n\,\theta) + \cos(m\,\theta).sen(n\,\theta).\ \nu' + sen(m\,\theta).\cos(n\,\theta).\ \nu' + \right.$$

$$\left. + sen(m\,\theta).sen(n\,\theta)\ .(\ \nu')^2\right) =$$

$$= |\, o \,|^{m+n} . \left(\cos(m\,\theta).\cos(n\,\theta) + \cos(m\,\theta).sen(n\,\theta).\ \nu' + sen(m\,\theta).\cos(n\,\theta).\ \nu' + \right.$$

$$\left. - sen(m\,\theta).sen(n\,\theta)\right) =$$

$$= |\, o \,|^{m+n} . \left(\cos(m\,\theta + n\,\theta) + sen(m\,\theta + n\,\theta).\ \nu'\right) =$$

$$= |\, o \,|^{m+n} . \left(\cos((m+n)\,\theta) + sen((m+n)\ \theta).\ \nu'\right) = o^{m+n}$$

3) Surge de expresar los octoniones o_1 , o_2 en forma trigonométrica, para luego efectuar el producto correspondiente. ■

Proposición 2.53

Sean $f(x) = \sum_{i=0}^{n} a_i . x^i$; $h(x) = \sum_{j=0}^{n} b_j . x^j$ *con* $a_i, b_j \in \mathbb{R}$ $\forall\ i\ ,\ j = 0, 1, \ldots, n$.

Sea o un octonión. Entonces

$$f\ (o)\ .\ h(o) = h(o)\ .\ f\ (o)$$

Demostración

$$f(o).\ h(o) = \left(\sum_{i=0}^{n} a_i . o^i\right).\left(\sum_{j=0}^{n} b_j . o^j\right) = \sum_{i=0}^{n}\ \sum_{j=0}^{n} \left(a_i . o^i\right).\ \left(b_j . o^j\right) =$$

$$\sum_{i=0}^{n}\ \sum_{j=0}^{n}\ \underbrace{\left(a_i . b_j\right).\left(o^i . o^j\right)}_{\text{Propos. 2.52, 3)}} = \sum_{i=0}^{n}\ \sum_{j=0}^{n}\ \left(a_i . b_j\right).\ \underbrace{o^{i+j}}_{\text{Propos. 2.52, 2)}} = \sum_{i=0}^{n}\ \sum_{j=0}^{n}\ \left(b_j . a_i\right).\ o^{i+j} =$$

$$= \underbrace{\sum_{j=0}^{n}\sum_{i=0}^{n}\left(b_j . a_i\right). o^{i+j}}_{\text{Conmutatividad de la suma en } O} \qquad [1]$$

Por otro lado,

$$h(o).f(o) = \left(\sum_{j=0}^{n} b_j . o^j\right).\left(\sum_{i=0}^{n} a_i . o^i\right) = \sum_{j=0}^{n}\sum_{i=0}^{n}\left(b_j . o^j\right).\left(a_i . o^i\right) = \sum_{j=0}^{n}\sum_{i=0}^{n} \underbrace{\left(b_j . a_i\right).\left(o^j . o^i\right)}_{\text{Propos. 2.52, 3)}} =$$

$$= \sum_{j=0}^{n}\sum_{i=0}^{n}\left(b_j . a_i\right). \underbrace{o^{j+i}}_{\text{Propos. 2.52, 2)}} = \sum_{j=0}^{n}\sum_{i=0}^{n}\left(b_j . a_i\right). o^{i+j} \qquad [2]$$

De [1] y [2] resulta que $f(o) \,.\, h(o) = h(o) \,.\, f(o)$. ■

Proposición 2.54

Sean $a,\ b \in O,\ m,\ n \in \mathbb{N}$. *Entonces*

1) $\left(a^n . a\right). b = a^n .(a \,.\, b)$

2) $\left(a^n . b\right). a^m = a^n .\left(b \,.\, a^m\right)$

3) $a \,.\, \left(b^n . b\right) = \left(a \,.\, b^n\right). b$

Demostración

1) Consideremos las representaciones trigonométricas de a y b. Es decir,

$$a = |\, a \,|\ \left(cos(\theta) + sen(\theta) \,.\, \nu'\right)$$

$$b = |\, b \,|\ \left(cos(\theta_1) + sen(\theta_1) \,.\, \nu_1'\right)$$

Entonces, por la Fórmula de De Moivre (Teorema *2.50*) y la Proposición *2.52* inciso *2*) tenemos:

$$a^n . a = |\, a \,|^{n+1}\ \left(cos\left((n+1)\theta\right) + sen\left((n+1)\theta\right) \,.\, \nu'\right)$$

Luego, aplicando la Proposición *2.52* inciso *3*) y la Propiedad Distributiva del producto respecto de la suma, resulta

$$\left(a^n . a\right). b = \left(|\, a \,|^{n+1}\ \left(cos\left((n+1)\theta\right) + sen\left((n+1)\theta\right) \,.\, \nu'\right)\right).\left(|\, b \,|\ \left(cos(\theta_1) + sen(\theta_1) \,.\, \nu_1'\right)\right) =$$

$$= |\, a \,|^{n+1} . |\, b \,|\ \left(\left(cos\left((n+1)\theta\right) + sen\left((n+1)\theta\right) \,.\, \nu'\right)\right).\left(\left(cos(\theta_1) + sen(\theta_1) \,.\, \nu_1'\right)\right) =$$

$$= |a|^{n+1} . |b| \left(\cos(n\theta+\theta)\cos(\theta_1) + \cos(n\theta+\theta)\,sen(\theta_1)\,\nu_1' + sen(n\theta+\theta)\cos(\theta_1)\nu' + sen(n\theta+\theta)\,sen(\theta_1)\nu'\nu_1' \right)$$

Por otro lado, teniendo en cuenta que

$$(\nu')^2 = (\nu_1')^2 = -1$$

Obtenemos

$$a^n.(a\,.\,b) = |a|^{n+1}|b| \left(\cos(n\theta)\cos(\theta)\cos(\theta_1) + \left(\cos(n\theta)\cos(\theta)sen(\theta_1)\nu_1' + \right.\right.$$

$$+\cos(n\theta)sen(\theta)\cos(\theta_1)\nu' + \cos(n\theta)sen(\theta)sen(\theta_1)\nu'\nu_1' + sen(n\theta)\cos(\theta)\cos(\theta_1)\nu' +$$

$$\left. +sen(n\theta)\cos(\theta)sen(\theta_1)\nu'\nu_1' + sen(n\theta)sen(\theta)\cos(\theta_1)(\nu')^2 + sen(n\theta)sen(\theta)sen(\theta_1)(\nu')^2\nu_1' \right) =$$

$$= |a|^{n+1} . |b| \left(\cos(n\theta+\theta)\cos(\theta_1) + \cos(n\theta+\theta)\,sen(\theta_1)\,\nu_1' + sen(n\theta+\theta)\cos(\theta_1)\nu' + sen(n\theta+\theta)\,sen(\theta_1)\nu'\nu_1' \right)$$

Por lo tanto, se verifica que

$$\left(a^n\,.\,a\right).\,b = a^n.(a\,.\,b)$$

2) y 3) se demuestran de manera similar ■

Proposición 2.55

Sean $f(x) = \sum_{i=0}^{k} a_i . x^i$; $h(x) = \sum_{j=0}^{k} b_j . x^j$ *con* $a_i, b_j \in \mathbb{R}$ $\forall\, i, j = 0, 1, \ldots, k$.

Sea $o \in O$ *un octonión. Entonces*

1) $\left[f(o)\right]^n . h(o) = h(o)\,.\left[f(o)\right]^n \quad \forall n \in \mathbb{N}$

2) $\left[f(o)\right]^n . \left[h(o)\right]^m = \left[h(o)\right]^m . \left[f(o)\right]^n \quad \forall n, m \in \mathbb{N}$

Demostración

1) Aplicaremos el Principio de Inducción sobre *n*.

Para *n = 1* se verifica, por la Proposición *2.53*.
Supongamos que la igualdad se verifica para *n*, es decir,

$$\left[f(o)\right]^n . h(o) = h(o)\,.\left[f(o)\right]^n$$

Veamos que la igualdad es válida para (*n+1*):

$$\left[f(o)\right]^{n+1} . h(o) = \left(\left[f(o)\right]^n . f(o)\right). h(o) = \left[f(o)\right]^n .\left(f(o).\,h(o)\right) = \left[f(o)\right]^n .\left(h(o).\,f(o)\right) =$$

Propos. 2.54, 1) *Propos. 2.53*

$$= \left(\left[f(o)\right]^n . h(o)\right). f(o) = \left(h(o).\left[f(o)\right]^n\right). f(o) = h(o).\left(\left[f(o)\right]^n . f(o)\right) = h(o)\,.\left[f(o)\right]^{n+1}$$

Propos. 2.54, 2) *Hipótesis Inductiva* *Propos. 2.54, 3)*

2) Aplicamos nuevamente el Principio de Inducción sobre *m*.
Para *m = 1* se verifica, por el inciso *1*).
Supongamos que la igualdad se verifica para *m*, es decir,

$$\left[f(o)\right]^n . \left[h(o)\right]^m = \left[h(o)\right]^m . \left[f(o)\right]^n$$

Veamos que se verifica para *(m+1):*

$$\left[f(o)\right]^n . \left[h(o)\right]^{m+1} = \left[f(o)\right]^n . \left(\left[h(o)\right]^m . h(o)\right) = \left(\left[f(o)\right]^n . \left[h(o)\right]^m\right) . h(o) =$$

Propos. 2.54, 3)

$$= \left(\left[h(o)\right]^m . \left[f(o)\right]^n\right) . h(o) = \left[h(o)\right]^m . \left(\left[f(o)\right]^n . h(o)\right) = \left[h(o)\right]^m . \left(h(o) \; . \left[f(o)\right]^n\right) =$$

Hipótesis Inductiva *Propos. 2.54, 2)* *Inciso 1)*

$$= \left(\left[h(o)\right]^m . h(o)\right) . \left[f(o)\right]^n = \left[h(o)\right]^{m+1} . \left[f(o)\right]^n \quad \blacksquare$$

Propos. 2.54, 1)

Proposición 2.56

Sean $f(x) = \sum_{i=0}^{k} a_i . x^i$; $h(x) = \sum_{j=0}^{k} b_j . x^j$ *con* $a_i, b_j \in \mathbb{R} \;\; \forall \; i, j = 0, 1, \ldots, k$.

Sean $o, w \in O$. *Entonces*

1) $w . \left(\left[f(o)\right]^n . \left[h(o)\right]^m\right) = \left(w . \left[f(o)\right]^n\right) . \left[h(o)\right]^m \quad \forall n, m \in \mathbb{N}$

2) $\left(\left[f(o)\right]^n . \left[h(o)\right]^m\right) . w = \left[f(o)\right]^n . \left(\left[h(o)\right]^m . w\right) \quad \forall n, m \in \mathbb{N}$

Demostración

Se demuestra de manera similar a la Proposición *2.54*, expresando en forma trigonométrica $w, f(o)$ y $h(o)$. ■

Propiedades que se pierden en el proceso de extensión de los números reales.

Al aplicarse el proceso de extensión de los reales para obtener los números complejos, se pierde la relación de orden. Al ampliar el conjunto de los números complejos al de los cuaterniones, se pierde la propiedad conmutativa. Y aplicando el proceso sobre el anillo de cuaterniones para generar los octoniones, se pierde la propiedad asociativa. Finalmente los octoniones pueden extenderse a un conjunto más amplio: el de los sediniones. Sin embargo, esta extensión hace que los sediniones formen un conjunto con divisores de cero, razón por la cual resulta poco interesante en Criptografía.

Capítulo 3

El algoritmo de Diffie-Hellman

En este capítulo analizaremos el Algoritmo de Diffie-Hellman, desarrollado en *1976* por Whitfield Diffie y Martin Hellman. Es utilizado para generar una clave secreta, la cual será compartida por dos personas. No se lo puede emplear para cifrar mensajes, conversaciones o firmas digitales.
Su seguridad radica en la extrema dificultad de calcular ciertos logaritmos discretos los cuales, hasta el día de hoy, constituyen un problema intratable para la Computación Clásica.
Este tipo de algoritmo pertenece a la rama de la Criptografía Asimétrica (o Criptografía de llave pública). Recordemos que ésta es una Criptografía que se basa en emplear dos claves: *una clave pública*, conocida por todo el mundo y *una clave privada*, conocida por una única persona. En el caso del Algoritmo de Diffie-Hellman, ambas claves se combinan para generar una clave secreta.

Procedimiento del algoritmo

Como mencionamos anteriormente, este algoritmo permite generar una clave secreta para ser compartida por dos personas, a las que llamaremos ***Alicia*** y ***Bernardo***. Consta de los siguientes pasos, diagramados en la siguiente figura:

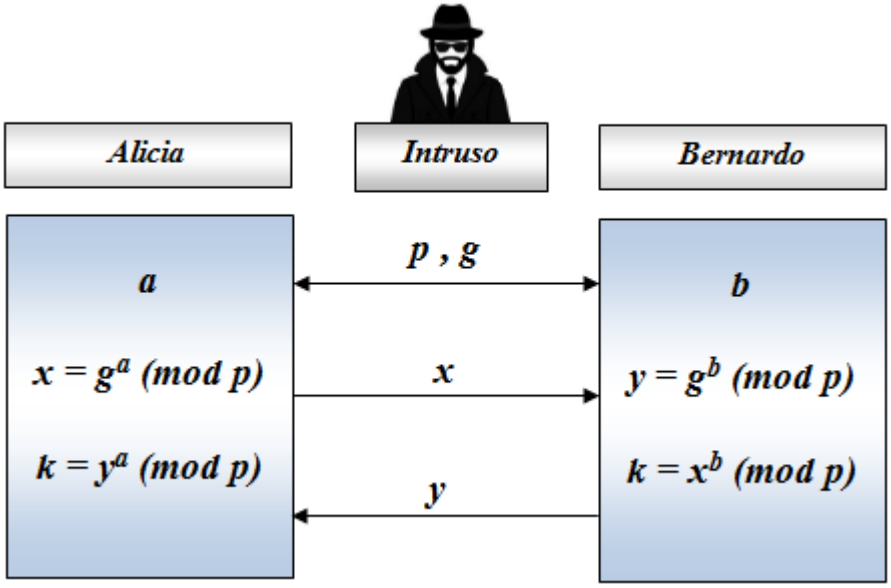


Figura 3.1: Diagrama que ilustra los pasos del Algoritmo de Diffie-Hellman.
Fuente imagen humana: https://sp.depositphotos.com/stock-photos/detective

Primer Paso

A través de un medio público (Internet por ejemplo) Alicia y Bernardo se ponen de acuerdo en usar un número primo ***p*** muy grande y un número ***g*** menor que ***p***. El "intruso" puede detectar ambos números.

Segundo Paso

Alicia escoge un número natural *"a"* menor que *p* que usará como exponente y lo mantiene en secreto. Bernardo hace lo propio, escoge un número natural *"b"* menor que ***p*** que usará como exponente y lo mantiene en secreto.

Tercer Paso

Con su exponente secreto Alicia calcula $x = g^a \pmod p$ y envía el valor *"x"* a Bernardo. De este modo, Bernardo conoce *"x"* pero no conoce *"a"*. Bernardo por su parte calcula $y = g^b \pmod p$ y envía el valor *"y"* a Alicia. De este modo, el intruso puede ver los resultados *"x"* e *"y"* pero no ve *"a"* ni *"b"*.

Cuarto Paso

Alicia recibe *"y"* y con su exponente secreto calcula $k = y^a \pmod p$.
Bernardo hace lo propio: recibe *"x"* y con su exponente secreto calcula $k = x^b \pmod p$. De este modo, Alicia y Bernardo comparten en forma secreta la misma clave ***k***.

Justificación de porqué Alicia y Bernardo obtienen la misma clave "k".

Como

$$y^a = \left(g^b\right)^a = g^{b.a} \pmod p$$

Y por otro lado

$$x^b = \left(g^a\right)^b = g^{a.b} = g^{b.a} \pmod p$$

Resulta entonces que $y^a = x^b = k \pmod p$.

Seguridad del Algoritmo de Diffie-Hellman

El intruso conoce ***p, g, x, y***. No conoce ***a*** ni ***b***. Conociendo $"a"$ podría descubrir la clave ***k*** ya que $y^a = k \pmod p$.

Como $g^a = x \pmod p$ entonces $a = log_g(x) \pmod p$ De este modo, para hallar $"a"$, el intruso debería calcular un logaritmo discreto. Para ello podría recurrir a la computadora y calcular las sucesivas potencias de g : $g^1, g^2, g^3, g^4, ...$ hasta que le dé ***x***. El Teorema de Euler asegura que dicho exponente es menor que $p-1.$ Pero si el primo ***p*** tiene más de *200* dígitos, el proceso puede tomar años.
Por esta razón, si el número primo ***p*** es suficientemente grande, el Algoritmo de Diffie-Hellman es muy seguro debido a que es prácticamente imposible descifrar su clave en un tiempo prudencial.

En el siguiente Ejemplo mostraremos cómo se implementa el protocolo Diffie-Hellman. El cálculo de las potencias modulares se realizará aplicando el algoritmo descripto en el Capítulo *2*.

Ejemplo 3.1

Primer Paso

Alicia y Bernardo acuerdan usar el número primo $p=2011$ y $g=100$.

Segundo Paso

Alicia escoge un número natural $a=144$ y no se lo revela a nadie.
Por otro lado, Bernardo escoge su exponente $b=812$ y tampoco se lo revela a nadie.

Tercer Paso

Con su exponente secreto Alicia calcula $x=g^a \pmod p$. Es decir, $x=100^{144}=1735 \pmod{2011}$ y envía *"1735"* a Bernardo.

Bernardo por su parte calcula $y=100^{812}=1431 \pmod{2011}$ y envía *"1431"* a Alicia.

Cuarto Paso

Alicia recibe *"y=1431"* y con su exponente secreto calcula $k=y^a \pmod p$.

Es decir, $k=1431^{144}=77 \pmod{2011}$.

Bernardo hace lo propio: recibe *"x=1735"* y con su exponente secreto calcula $k=x^b \pmod p$.O sea, $k=1735^{812}=77 \pmod{2011}$. De este modo, Alicia y Bernardo comparten en forma secreta la misma clave ***k =77***.

El intruso conoce $p=2011$, $g=100$, $x=1735$, $y=1431$. Su problema es hallar $a=log_g(x) \pmod p$ ó $b=log_g(y) \pmod p$. Con un número ***p*** de *4* cifras, el algoritmo que calcula las potencias modulares expuestas en el Capítulo *2* puede dar la respuesta. Pero si ***p*** tuviera *100* cifras o más, el cálculo de cualquiera de los dos logaritmos sería muy costoso en términos de tiempo.

El próximo Ejemplo mostraremos cómo el "intruso" podría llegar a descubrir fácilmente la clave secreta si el número *p* fuera pequeño.

Ejemplo 3.2

Un intruso navega por los portales de Alicia y Bernardo y en ambos halla $p=17$ y $g=9$. Luego, ve el misterioso número *15* en la página de Bernardo y el misterioso número *2* en la de Alicia. ¿Podría el intruso determinar el número secreto que Alicia y Bernardo comparten?

Solución

Se sabe que $p = 17$ y $g = 9$. También que $x = 2$ e $y = 15$. Entonces, el intruso procede a calcular ***a*** ó ***b***. Supongamos que decide hallar ***a***. Como ***a*** verifica que

$$g^a = x \pmod{p} \Rightarrow 9^a = 2 \pmod{17}$$

Por lo tanto, el intruso calculará las potencias modulares $9^i \pmod{17}$ hasta encontrar un "a" tal que $9^a = 2 \pmod{17}$. La siguientes tablas muestran estas potencias modulares:

i	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***
$9^i \pmod{17}$	***9***	***13***	***15***	***16***	***8***	***4***	***2***	***1***

i	***9***	***10***	***11***	***12***	***13***	***14***	***15***	***16***
$9^i \pmod{17}$	***9***	***13***	***15***	***16***	***8***	***4***	***2***	***1***

Al observar estas tablas, el intruso deduce que $a = 7$ *ó* $a = 15$.
Luego, calcula la clave ***k*** que Alicia y Bernardo comparten, del siguiente modo:
$k = y^a = 15^7 = 8 \pmod{17}$ ó $k = y^a = 15^{15} = 8 \pmod{17}$
Por lo tanto, el número secreto que Alicia y Bernardo comparten es $k = 8$.

Capítulo 4

El algoritmo de Diffie-Hellman aplicando estructuras algebraicas no conmutativas

Uno de los inconvenientes que presenta el Algoritmo de Diffie-Hellman es que necesita emplear bibliotecas de precisión extendida y un hardware con alta capacidad computacional. Porque para garantizar la seguridad de dicho algoritmo, es necesario que el número primo *p* sea muy grande. Por esta razón los autores Pedro Hecht y Jorge Kamlofsky propusieron una modificación del Protocolo de Diffie-Hellman utilizando estructuras algebraicas no conmutativas, como lo son los cuaterniones y los octoniones. Estos métodos criptográficos otorgan un gran beneficio, ya que pueden ser ejecutados en procesadores de bajo poder computacional y memoria RAM reducida, como por ejemplo, en tarjetas inteligentes o teléfonos celulares. En este capítulo desarrollaremos las dos variantes del Protocolo de Diffie-Hellman propuestos por Hecht y Kamlofsky: aplicando cuaterniones y luego utilizando octoniones.

1. Algoritmo de Diffie-Hellman aplicando cuaterniones

En esta sección presentamos una variación del algoritmo Diffie-Hellman aplicando el anillo no conmutativo de los cuaterniones.

Procedimiento del algoritmo

Alicia y Bernardo generarán una clave de seguridad para ser compartida. Los pasos a seguir se diagraman en el siguiente gráfico:

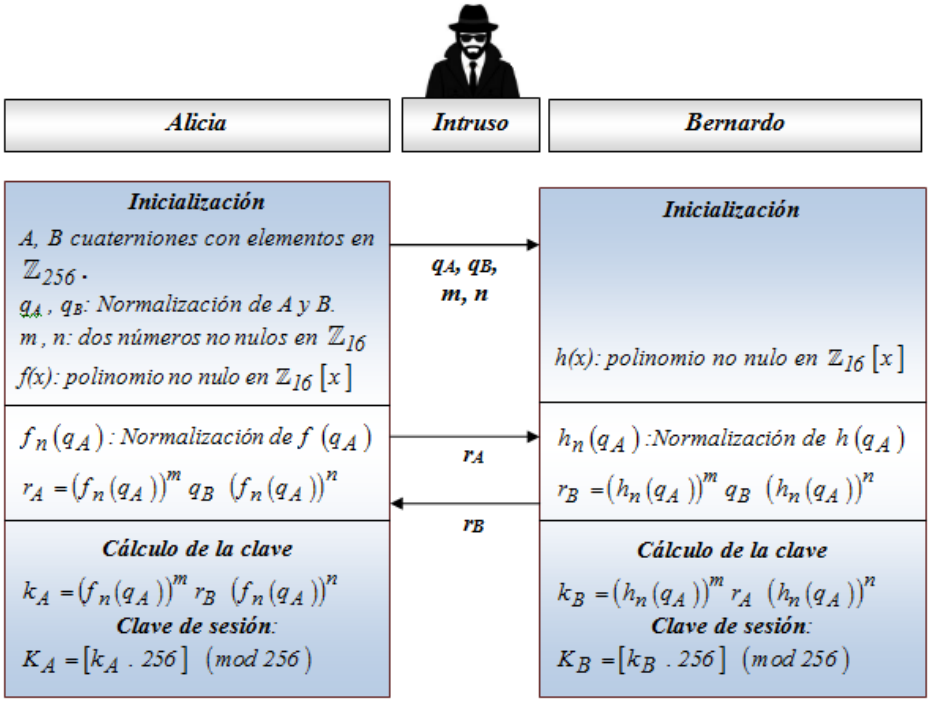


Figura 4.1: Diagrama que ilustra los pasos del Algoritmo de Diffie-Hellman aplicando cuaterniones.

Primer Paso

Alicia elige dos cuaterniones *A* y *B* no nulos, a coeficientes en $\mathbb{Z}_{256}$. Además, elige dos elementos no nulos *m* y *n* pertenecientes a $\mathbb{Z}_{16}$.

Segundo Paso

Alicia calcula la normalización de A y B, es decir, $q_A = \frac{A}{|A|}$ y $q_B = \frac{B}{|B|}$.

Tercer Paso

Alicia elige como clave privada un polinomio $f(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$ y tal que $f(q_A) \neq 0$.

Cuarto Paso

Alicia envía a Bernardo q_A , q_B , m y n por un canal inseguro.

Quinto Paso

Bernardo elige como clave privada un polinomio $h(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$ y tal que $h(q_A) \neq 0$.

Sexto Paso

Alicia calcula

$$f_n(q_A) = \frac{f(q_A)}{|f(q_A)|}$$

$$r_A = (f_n(q_A))^m \, q_B \, (f_n(q_A))^n$$

Y envía a Bernardo el valor de r_A por un canal inseguro.

Séptimo Paso

Bernardo calcula

$$h_n(q_A) = \frac{h(q_A)}{|h(q_A)|}$$

$$r_B = (h_n(q_A))^m \, q_B \, (h_n(q_A))^n$$

Y envía a Alicia el valor de r_B por un canal inseguro.

Cálculo de claves

Octavo Paso

Alicia calcula su clave

$$k_A = (f_n(q_A))^m \, r_B \, (f_n(q_A))^n .$$

Por otro lado, Bernardo calcula su clave

$$k_B = \left(h_n\left(q_A\right)\right)^m r_A \ \left(h_n\left(q_A\right)\right)^n .$$

Se puede verificar, como se demostrará en la Proposición *4.5.7*, que

$$k_A = k_B .$$

Noveno Paso

A fin de que las componentes de k_A y k_B, que son cuaterniones, sean elementos de $\mathbb{Z}_{256}$, se consideran como claves a

$$K_A = \left[k_A \ . 256\right] \ \left(mod\ 256\right)$$
$$K_B = \left[k_B \ . 256\right] \ \left(mod\ 256\right)$$

Donde $\left[k_A \ . 256\right]$ y $\left[k_B \ . 256\right]$ son los números que se obtienen de truncar, respectivamente, la parte decimal de $k_A \ . 256$ y de $k_B \ . 256$. Mientras que K_A y K_B son los restos de la división entera de $\left[k_A \ . 256\right]$ y $\left[k_B \ . 256\right]$ por *256*.

Justificación de porqué Alicia y Bernardo obtienen la misma clave.

De la Proposición *2.43* inciso *2*) *b*) y aplicando la Propiedad Asociativa del producto entre cuaterniones, resulta

$$k_B = \left[h_n\left(q_A\right)\right]^m \ . r_A \ . \left[h_n\left(q_A\right)\right]^n = \left[h_n\left(q_A\right)\right]^m \ . \left[f_n\left(q_A\right)\right]^m \ . q_B \ . \left[f_n\left(q_A\right)\right]^n \ . \left[h_n\left(q_A\right)\right]^n =$$
$$= \left[f_n\left(q_A\right)\right]^m \ . \left[h_n\left(q_A\right)\right]^m \ . q_B \ . \left[h_n\left(q_A\right)\right]^n \ . \left[f_n\left(q_A\right)\right]^n = k_A$$

Observación

Las normalizaciones realizadas permiten que el cálculo de las potencias de cuaterniones se limite a multiplicaciones del argumento de *senos* y *cosenos* por el valor del exponente, logrando de este modo operaciones más sencillas, manteniendo además la esencia del cuaternión original.

El siguiente Ejemplo numérico mostraremos cómo generar una clave en el Algoritmo de Diffie-Hellman aplicando cuaterniones.

Ejemplo 4.1

Primer Paso

Alicia elige dos cuaterniones *A* y *B* no nulos, a coeficientes en $\mathbb{Z}_{256}$.

$$A = (2,2,2,2)$$
$$B = (3,0,4,0)$$

Además, elige dos elementos no nulos *m* y *n* pertenecientes a $\mathbb{Z}_{16}$.

$$m = 3$$
$$n = 2$$

Segundo Paso

Alicia calcula la normalización de A y B, es decir, $q_A = \frac{A}{|A|}$ y $q_B = \frac{B}{|B|}$.

$$q_A = \frac{A}{|A|} = \frac{(2,2,2,2)}{\sqrt{2^2+2^2+2^2+2^2}} = \left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$$

$$q_B = \frac{B}{|B|} = \frac{(3,0,4,0)}{\sqrt{3^2+0^2+4^2+0^2}} = \left(\frac{3}{5},0,\frac{4}{5},0\right)$$

Tercer Paso

Alicia elige como clave privada un polinomio $f(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$ y tal que $f(q_A) \neq 0$:

$$f(x) = 2x^5 + 3x^4$$

Cuarto Paso

Alicia envía a Bernardo q_A, q_B, m y n por un canal inseguro.

Quinto Paso

Bernardo elige como clave privada un polinomio $h(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$ y tal que $h(q_A) \neq 0$:

$$h(x) = 3x^6 + 4x^8$$

Sexto Paso

Alicia calcula

$$f_n(q_A) = \frac{f(q_A)}{|f(q_A)|}$$

$$r_A = (f_n(q_A))^m \, q_B \, (f_n(q_A))^n$$

Y envía a Bernardo el valor de r_A por un canal inseguro. Para ello se expresa primeramente q_A en forma trigonométrica:

$$q_A = |q_A| \,.\, (\cos(\theta) + sen(\theta).v')$$

$$|q_A| = 1 \ ,$$

$$\theta = arccos\left(\frac{a}{|q_A|}\right) = arccos\left(\frac{\frac{1}{2}}{1}\right) = arccos\left(\frac{1}{2}\right) = \frac{\pi}{3} \ ,$$

$$v' = \frac{(b,c,d)}{|(b,c,d)|} = \frac{\left(\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)}{\left|\left(\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)\right|} = \frac{\left(\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)}{\sqrt{\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2}} = \frac{\left(\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)}{\sqrt{\frac{1}{4}+\frac{1}{4}+\frac{1}{4}}} =$$

$$= \frac{\left(\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)}{\sqrt{\frac{3}{4}}} = \left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right)$$

Por lo tanto:

$$q_A = cos\left(\frac{\pi}{3}\right) + sen\left(\frac{\pi}{3}\right).v' \ .$$

Entonces, aplicando la fórmula de De Moivre, resulta:

$$f(q_A) = 2.q_A^5 + 3.q_A^4 = 2.\left[cos\left(\frac{5\pi}{3}\right) + sen\left(\frac{5\pi}{3}\right).v'\right] + 3.\left[cos\left(\frac{4\pi}{3}\right) + sen\left(\frac{4\pi}{3}\right).v'\right] =$$

$$= 2.\left[\frac{1}{2} - \frac{\sqrt{3}}{2}.\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right)\right] + 3.\left[-\frac{1}{2} - \frac{\sqrt{3}}{2}.\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right)\right] =$$

$$= 2.\left[\frac{1}{2} + \left(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}\right)\right] + 3.\left[-\frac{1}{2} + \left(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}\right)\right] =$$

$$= 1 + (-1,-1,-1) - \frac{3}{2} + \left(-\frac{3}{2},-\frac{3}{2},-\frac{3}{2}\right) = 1 - i - j - k - \frac{3}{2} - \frac{3}{2}i - \frac{3}{2}j - \frac{3}{2}k =$$

$$= -\frac{1}{2} - \frac{5}{2}i - \frac{5}{2}j - \frac{5}{2}k$$

Luego

$$f(q_A) = -\frac{1}{2} - \frac{5}{2}i - \frac{5}{2}j - \frac{5}{2}k \ .$$

Y también se tiene que:

$$f_n(q_A) = \frac{f(q_A)}{|f(q_A)|} = \frac{\left(-\frac{1}{2},-\frac{5}{2},-\frac{5}{2},-\frac{5}{2}\right)}{\left|\left(-\frac{1}{2},-\frac{5}{2},-\frac{5}{2},-\frac{5}{2}\right)\right|} = \frac{\left(-\frac{1}{2},-\frac{5}{2},-\frac{5}{2},-\frac{5}{2}\right)}{\sqrt{\left(-\frac{1}{2}\right)^2+\left(-\frac{5}{2}\right)^2+\left(-\frac{5}{2}\right)^2+\left(-\frac{5}{2}\right)^2}} =$$

$$= \frac{\left(-\frac{1}{2},-\frac{5}{2},-\frac{5}{2},-\frac{5}{2}\right)}{\sqrt{\frac{1}{4}+3.\frac{25}{4}}} = \frac{\left(-\frac{1}{2},-\frac{5}{2},-\frac{5}{2},-\frac{5}{2}\right)}{\sqrt{19}} = \left(-\frac{1}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}}\right)$$

A continuación expresamos $f_n(q_A)$ en forma trigonométrica:

$$f_n(q_A) = |f_n(q_A)| \ . \ \left(cos(\theta) + sen(\theta).v'\right)$$

Entonces

$$|f_n(q_A)| = 1$$

Para calcular θ y v' consideramos dos decimales:

$$\theta = arccos\left(\frac{a}{|f_n(q_A)|}\right) = arccos\left(-\frac{1}{2\sqrt{19}}\right) = 1,69 \ ,$$

$$v' = \frac{(b,c,d)}{|(b,c,d)|} = \frac{\left(-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}}\right)}{\left|\left(-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}}\right)\right|} =$$

$$= \frac{\left(-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}}\right)}{\sqrt{\left(-\frac{5}{2\sqrt{19}}\right)^2+\left(-\frac{5}{2\sqrt{19}}\right)^2+\left(-\frac{5}{2\sqrt{19}}\right)^2}} =$$

$$= \frac{\left(-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}}\right)}{\sqrt{3.\frac{25}{76}}} = \frac{\left(-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}},-\frac{5}{2\sqrt{19}}\right)}{\sqrt{\frac{75}{76}}} =$$

$$= \left(-\frac{5}{\sqrt{75}},-\frac{5}{\sqrt{75}},-\frac{5}{\sqrt{75}}\right)$$

Por lo tanto:

$$f_n(q_A) = cos(1,69) + sen(1,69).v'$$

Finalmente calculamos r_A:

$$r_A = \left[f_n(q_A)\right]^m \cdot q_B \cdot \left[f_n(q_A)\right]^n =$$

$$= \left[cos\left(3.(1,69)\right) + sen\left(3.(1,69)\right).v'\right].\left(\frac{3}{5},0,\frac{4}{5},0\right).\left[cos\left(2.(1,69)\right) + sen\left(2.(1,69)\right).v'\right] =$$

$$= (0,06145 \ , 0,05370 \ , -0,4969 \ , -0,8640)$$

Es decir,

$$r_A = (0,06145 \ , 0,05370 \ , -0,4969 \ , -0,8640)$$

Séptimo Paso

Bernardo calcula

$$h_n(q_A) = \frac{h(q_A)}{|h(q_A)|}$$

$$r_B = \left(h_n(q_A)\right)^m q_B \ \left(h_n(q_A)\right)^n$$

Y envía a Alicia el valor de r_B por un canal inseguro.

Entonces

$$h(q_A) = 3.q_A^6 + 4.\ q_A^8 = 3.\left[cos(2\pi) + sen(2\pi).\ v'\right] + 4.\left[cos\left(\frac{8\pi}{3}\right) + sen\left(\frac{8\pi}{3}\right).\ v'\right] =$$

$$= 3.[1-0] + 4.\left[-\frac{1}{2} + \frac{\sqrt{3}}{2}.\left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right)\right] = 3 + 4.\left[-\frac{1}{2} + \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)\right] =$$

$$= 3 - 2 + (2,2,2) = 3 - 2 + 2i + 2j + 2k = 1 + 2i + 2j + 2k$$

Luego

$$h_n(q_A) = \frac{h(q_A)}{|h(q_A)|} = \frac{(1,2,2,2)}{|(1,2,2,2)|} = \frac{(1,2,2,2)}{\sqrt{1^2 + 2^2 + 2^2 + 2^2}} =$$

$$= \frac{(1,2,2,2)}{\sqrt{13}} = \left(\frac{1}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)$$

A continuación expresamos $h_n(q_A)$ en forma trigonométrica:

$$h_n(q_A) = |h_n(q_A)|\ .\ \left(cos(\theta) + sen(\theta).\ v'\right)\ .$$

Entonces

$$|h_n(q_A)| = 1\ .$$

Calculamos θ y v' considerando dos decimales

$$\theta = arccos\left(\frac{a}{|h_n(q_A)|}\right) = arccos\left(\frac{1}{\sqrt{13}}\right) = 1,29\ ,$$

$$v' = \frac{(b,c,d)}{|(b,c,d)|} = \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\left|\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)\right|} = \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\sqrt{\left(\frac{2}{\sqrt{13}}\right)^2 + \left(\frac{2}{\sqrt{13}}\right)^2 + \left(\frac{2}{\sqrt{13}}\right)^2}} =$$

$$= \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\sqrt{3.\frac{4}{13}}} = \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\sqrt{\frac{12}{13}}} = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right)$$

Por lo tanto:

$$h_n(q_A) = cos(1,29) + sen(1,29).\ v'$$

Finalmente calculamos r_B :

$$r_B = \left[h_n(q_A)\right]^m\ .\ q_b\ .\ \left[h_n(q_A)\right]^n =$$

$$= \left[cos\left(3.(1,29)\right) + sen\left(3.(1,29)\right).\ v'\right].\left(\frac{3}{5}, 0, \frac{4}{5}, 0\right).\left[cos\left(2.(1,29)\right) + sen\left(2.(1,29)\right).\ v'\right] =$$

$$= (0,5156\ ,\ -0,1976\ ,\ 0,4680\ ,\ 0,6899)$$

Es decir,

$$r_B = (0,5156\ ,\ -0,1976\ ,\ 0,4680\ ,\ 0,6899)$$

Cálculo de claves

Octavo Paso

Alicia calcula su clave k_A

$$k_A = (f_n(q_A))^m\ r_B\ (f_n(q_A))^n .$$

Es decir,

$$k_A = [f_n(q_A)]^m . r_B . [f_n(q_A)]^n =$$

$$= [cos(3.(1.69)) + sen(3.(1.69))v'] . r_B . [cos(2.(1.69)) + sen(2.(1.69))v'] =$$

$$= (0,185\ ,\ -0,492\ ,\ 0,068\ ,\ -0,848)$$

Por lo tanto

$$k_A = (0,185\ ,\ -0,492\ ,\ 0,068\ ,\ -0,848)$$

Por otro lado, Bernardo calcula su clave

$$k_B = (h_n(q_A))^m\ r_A\ (h_n(q_A))^n .$$

Entonces

$$k_B = [h_n(q_A)]^m . r_A . [h_n(q_A)]^n =$$

$$= [cos(3.(1.29)) + sen(3.(1.29))v'] . r_A . [cos(2.(1.29)) + sen(2.(1.29))v'] =$$

$$= (0,185\ ,\ -0,492\ ,\ 0,068\ ,\ -0,848)$$

En consecuencia

$$k_B = (0,185\ ,\ -0,492\ ,\ 0,068\ ,\ -0,848)$$

Noveno Paso

A fin de que las componentes de k_A y k_B tenga sus elementos en $\mathbb{Z}_{256}$, se consideran como claves a

$$K_A = [k_A . 256]\ \ (mod\ 256)$$

$$K_B = [k_B . 256]\ \ (mod\ 256)$$

Es decir

$$K_A = K_B = [(0.185,-0.492,0.068,-0.848).256] = [(47.36,-125.952,17.408,-217.088)] =$$

$$= (47,-125,17,-217) \equiv (47,131,17,39)\ \ (mod\ 256)$$

De este modo,

$$K_A = K_B = (47,131,17,39)\ \ (mod\ 256)$$

2. Algoritmo de Diffie-Hellman aplicando octoniones

Este algoritmo, llamado el Protocolo *HK17*, aplica el Algoritmo de Diffie-Hellman empleando octoniones.

Procedimiento del algoritmo

Alicia y Bernardo generarán una clave de seguridad para ser compartida. Los pasos a seguir figuran en el siguiente diagrama:

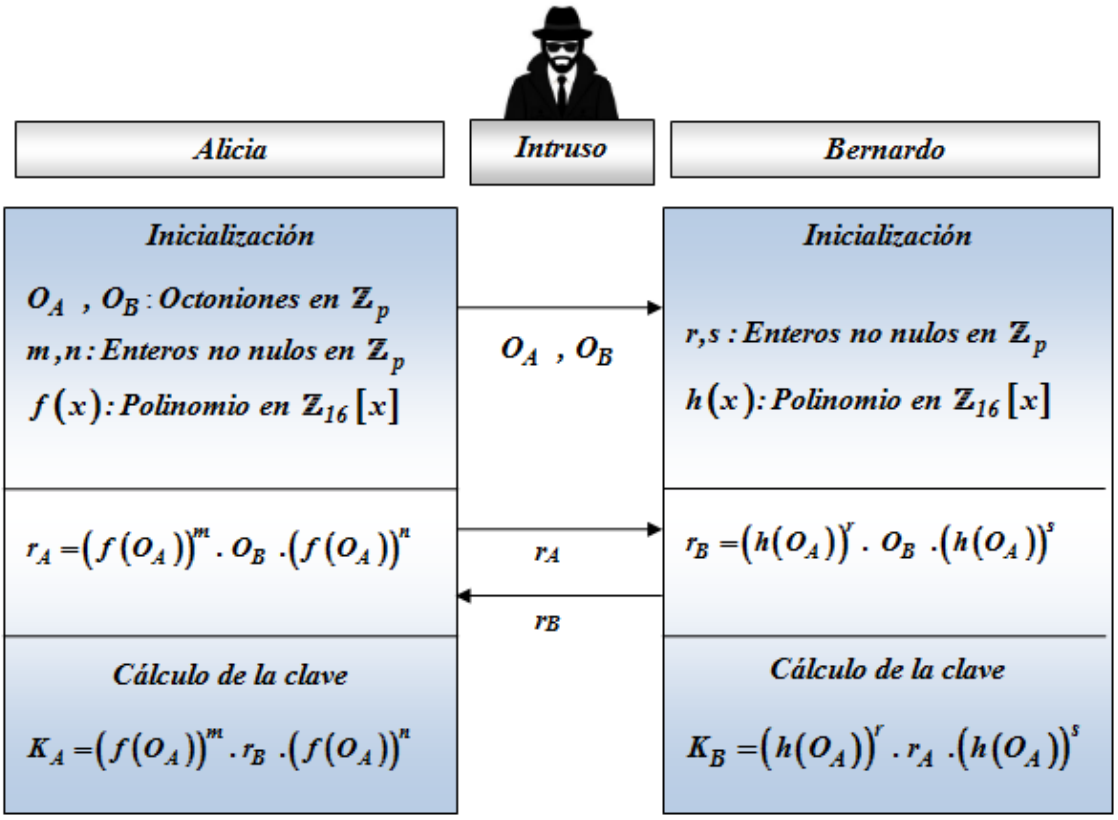


Figura 4.3: Diagrama que ilustra los pasos del Algoritmo de Diffie-Hellman aplicando octoniones.

Primer Paso

Alicia elige dos octoniones O_A y O_B, con elementos en $\mathbb{Z}_p$, para algún primo p.

Segundo Paso

Alicia elige como clave privada dos enteros $m, n \in \mathbb{Z}_p$ y un polinomio no nulo $f(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$, tal que $f(O_A) \neq 0$. Luego envía a Bernardo O_A y O_B por un canal inseguro.

Tercer Paso

Bernardo elige como clave privada dos enteros $r, s \in \mathbb{Z}_p$ y un polinomio no nulo $h(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$, tal que $h(O_A) \neq 0$.

Cuarto Paso

Alicia calcula

$$r_A = \left[f(O_A) \right]^m . O_B . \left[f(O_A) \right]^n$$

Y lo envía a Bernardo. Por otro lado, Bernardo calcula

$$r_B = \left[h(O_A) \right]^r . O_B . \left[h(O_A) \right]^s$$

Y lo envía a Alicia por un canal inseguro.

Quinto Paso

Alicia calcula su clave

$$K_A = \left[f(O_A) \right]^m . r_B . \left[f(O_A) \right]^n$$

Por otro lado, Bernardo calcula su clave

$$K_B = \left[h(O_A) \right]^r . r_A . \left[h(O_A) \right]^s$$

Finalmente, Alicia y Bernardo comparten la clave

$$K_A = K_B$$

Justificación de porqué Alicia y Bernardo obtienen la misma clave.

$$K_A = \left[f(O_A) \right]^m . r_B . \left[f(O_A) \right]^n = \left[f(O_A) \right]^m . \left(\left[h(O_A) \right]^r . \underbrace{O_B . \left[h(O_A) \right]^s}_{w} \right) . \left[f(O_A) \right]^n =$$

Proposición 2.56, 2)

$$= \left(\left[f(O_A) \right]^m . \left[h(O_A) \right]^r \right) . O_B . \left[h(O_A) \right]^s . \left[f(O_A) \right]^n =$$

Proposición 2.55, 2)

$$= \left(\left[h(O_A) \right]^r . \left[f(O_A) \right]^m \right) . \underbrace{O_B . \left[h(O_A) \right]^s}_{w} . \left[f(O_A) \right]^n =$$

Proposición 2.56, 2)

$$= \left[h(O_A) \right]^r . \left(\underbrace{\left[f(O_A) \right]^m . O_B}_{w} . \left[h(O_A) \right]^s \right) . \left[f(O_A) \right]^n =$$

Proposición 2.56, 1)

$$= \left[h(O_A) \right]^r . \underbrace{\left[f(O_A) \right]^m . O_B}_{w} . \left(\left[h(O_A) \right]^s . \left[f(O_A) \right]^n \right) =$$

Proposición 2.55, 2)

$$= \left[h(O_A)\right]^r \cdot \underbrace{\left[f(O_A)\right]^m \cdot O_B}_{w} \cdot \left(\left[f(O_A)\right]^n \cdot \left[h(O_A)\right]^s\right) =$$

Proposición 2.56, 1)

$$= \left[h(O_A)\right]^r \cdot \left(\left[f(O_A)\right]^m \cdot O_B \cdot \left[f(O_A)\right]^n\right) \cdot \left[h(O_A)\right]^s = \left[h(O_A)\right]^r \cdot r_A \cdot \left[h(O_A)\right]^s = K_B$$

Observación

En este algoritmo, las operaciones entre octoniones se realizan en $\mathbb{Z}_p$, considerando la suma y producto de octoniones definidos en el Capítulo anterior. Es decir, si $O_1 = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ y $O_2 = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)$ son dos octoniones, entonces

$$O_1 + O_2 = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4, a_5 + b_5, a_6 + b_6, a_7 + b_7)$$

$$O_1 \cdot O_2 =$$

$$\begin{aligned}
&(a_0\, b_0 - a_1\, b_1 - a_2\, b_2 - a_3\, b_3 - a_4\, b_4 - a_5\, b_5 - a_6\, b_6 - a_7\, b_7,\\
&a_0\, b_1 + a_1\, b_0 + a_2\, b_4 + a_3\, b_7 - a_4\, b_2 + a_5\, b_6 - a_6\, b_5 - a_7\, b_3,\\
&a_0\, b_2 - a_1\, b_4 + a_2\, b_0 + a_3\, b_5 + a_4\, b_1 - a_5\, b_3 + a_6\, b_7 - a_7\, b_6,\\
&a_0\, b_3 - a_1\, b_7 - a_2\, b_5 + a_3\, b_0 + a_4\, b_6 + a_5\, b_2 - a_6\, b_4 + a_7\, b_1,\\
&a_0\, b_4 + a_1\, b_2 - a_2\, b_1 - a_3\, b_6 + a_4\, b_0 + a_5\, b_7 + a_6\, b_3 - a_7\, b_5,\\
&a_0\, b_5 - a_1\, b_6 + a_2\, b_3 - a_3\, b_2 - a_4\, b_7 + a_5\, b_0 + a_6\, b_1 + a_7\, b_4,\\
&a_0\, b_6 + a_1\, b_5 - a_2\, b_7 + a_3\, b_4 - a_4\, b_3 - a_5\, b_1 + a_6\, b_0 + a_7\, b_2,\\
&a_0\, b_7 + a_1\, b_3 + a_2\, b_6 - a_3\, b_1 + a_4\, b_5 - a_5\, b_4 - a_6\, b_2 + a_7\, b_0)
\end{aligned}$$

Donde las operaciones de suma y producto involucradas en cada componente se efectúan en $\mathbb{Z}_p$. En el siguiente Ejemplo mostraremos cómo generar una clave empleando este algoritmo.

Ejemplo 4.2

Alicia y Bernardo deciden crear una clave para ser compartida entre ambos, utilizando el Algoritmo de Diffie-Hellman basado en octoniones. Para ello ejecutan los siguientes pasos:

Primer Paso

Alicia elige dos octoniones O_A y O_B, con elementos en $\mathbb{Z}_p$, considerando $p = 13$:

$$O_A = (1, 2, 10, 0, 0, 5, 11, 0)$$

$$O_B = (3, 0, 9, 1, 0, 1, 0, 0)$$

Segundo Paso

Alicia elige como clave privada dos enteros *m=2*, *n=3* y un polinomio no nulo $f(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$, definido por $f(x)=3x^3+2x$. Luego envía a Bernardo O_A y O_B por un canal inseguro.

Tercer Paso

Bernardo elige como clave privada dos enteros *r = 2*, *s = 2* y un polinomio no nulo $h(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$, definido por $h(x)=2x^4$.

Cuarto Paso

Alicia calcula

$$r_A=\left[f(O_A)\right]^m . O_B .\left[f(O_A)\right]^n$$

Para ello efectúa las siguientes operaciones:

$$f(O_A)=3(O_A)^3+2O_A=3.(1,\ 2,\ 10,\ 0,\ 0,\ 5,\ 11,\ 0)^3+2.(1,\ 2,\ 10,\ 0,\ 0,\ 5,\ 11,\ 0)=$$

$$=3.(5,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0)+2.(1,\ 2,\ 10,\ 0,\ 0,\ 5,\ 11,\ 0)=(17,\ 4,\ 20,\ 0,\ 0,\ 10,\ 22,\ 0)\equiv$$

$$\equiv(4,\ 4,\ 7,\ 0,\ 0,\ 10,\ 9,\ 0)$$

Luego

$$f(O_A)=(4,\ 4,\ 7,\ 0,\ 0,\ 10,\ 9,\ 0)\ \ en\ \mathbb{Z}_{13}$$

Entonces

$$r_A=\left[f(O_A)\right]^m . O_B .\left[f(O_A)\right]^n=(4,4,7,0,0,10,9,0)^2.(3,\ 0,\ 9,\ 1,\ 0,\ 1,\ 0,\ 0).(4,4,7,0,0,10,9,0)^3=$$

$$=(4,6,4,0,0,2,7,0).(3,\ 0,\ 9,\ 1,\ 0,\ 1,\ 0,\ 0).(11,1,5,0,0,9,12,0)=(11,\ 1\ ,9\ ,9\ ,2\ ,11\ ,6\ ,\ 9)$$

Es decir

$$r_A=(11,\ 1\ ,9\ ,9\ ,2\ ,11\ ,6\ ,\ 9)$$

Alicia envía este octonión a Bernardo. Por otro lado, Bernardo calcula

$$r_B=\left[h(O_A)\right]^r . O_B .\left[h(O_A)\right]^s$$

Para ello calculamos primero

$$h(O_A)=2(O_A)^4=2.(1,\ 2,\ 10,\ 0,\ 0,\ 5,\ 11,\ 0)^4=2.(5,\ 10,\ 11,\ 0,\ 0,\ 12,\ 3,\ 0)=$$

$$=(10,\ 20,\ 22,\ 0,\ 0,\ 24,\ 6,\ 0)\equiv(10,7,9,0,0,11,6,0)$$

Entonces

$$h(O_A)=(10,7,9,0,0,11,6,0)$$

Por lo tanto

$$r_B = \left[h(O_A)\right]^r . O_B . \left[h(O_A)\right]^s = (10,7,9,0,0,11,6,0)^2 . (3,\ 0,\ 9,\ 1,\ 0,\ 1,\ 0,\ 0)\ . (10,7,9,0,0,11,6,0)^2 =$$

$$= (8,10,11,0,0,12,3,0).(3,\ 0,\ 9,\ 1,\ 0,\ 1,\ 0,\ 0)\ . (8,10,11,0,0,12,3,0) = (11,2,0,9,0,1,11,0)$$

Es decir

$$r_B = (11,2,0,9,0,1,11,0)$$

Quinto Paso

Alicia calcula su clave

$$K_A = \left[f(O_A)\right]^m . r_B . \left[f(O_A)\right]^n = (4,4,7,0,0,10,9,0)^2 . (11,2,0,9,0,1,11,0).(4,4,7,0,0,10,9,0)^3 =$$

$$= (12,8,11,3,5,12,3,3)$$

Es decir

$$K_A = (12,8,11,3,5,12,3,3)$$

Por otro lado, Bernardo calcula su clave

$$K_B = \left[h(O_A)\right]^r . r_A . \left[h(O_A)\right]^s = (10,7,9,0,0,11,6,0)^2 . (5,12,2,7,11,11,9,3)\ . (10,7,9,0,0,11,6,0)^2 =$$

$$= (12,8,11,3,5,12,3,3)$$

Luego

$$K_B = (12,8,11,3,5,12,3,3)$$

Finalmente, Alicia y Bernardo comparten la clave

$$K_A = K_B$$

Los métodos criptográficos descriptos en este Capítulo son llamados *compactos* debido a que, para su funcionamiento, no requieren de librerías de precisión extendida. Más aún, los protocolos presentados sólo realizan operaciones de suma y producto, lo que permite que sea aplicable a procesadores muy simples y de bajo porte.

En el caso del Algoritmo de Diffie-Hellman aplicando cuaterniones, la clave resultante es un vector de *4* elementos en $\mathbb{Z}_{256}$, conformando así una clave de *32* bits (pues cada número en $\mathbb{Z}_{256}$ ocupa a lo sumo 8 bits), adecuada para su uso en sistemas de cifrado simétrico tipo AES (véase Referencia [4]).

Por otro lado, si se aplican octoniones, el tiempo requerido para generar claves es algo mayor que si se aplicaran cuaterniones, pero suele ser más robusto debido a que los octoniones no gozan de la propiedad asociativa (véase Referencia [4]).

Estos algoritmos fueron considerados muy seguros. Sin embargo, en *2019* se diseñó un método de ataque que permitió descifrar las claves generadas por estos protocolos. Esto lo veremos en el Capítulo siguiente.

Capítulo 5

Descifrado de la clave del Protocolo HK17

En este Capítulo desarrollaremos el algoritmo de ataque propuesto por los autores Haoyu, Renzhang, Qutaibah, Yanbin, Yongge y Tianyuan, que permitirá descifrar la clave generada por el Protocolo HK17, como así también la de *Diffie-Hellman* que aplica cuaterniones.

1. Descifrado de la clave del Protocolo HK17

Primeramente enunciaremos las siguientes Definiciones y Proposiciones que utilizaremos para justificar el procedimiento que descifra la clave generada por este algoritmo.

Teorema 5.1: División de polinomios en $\mathbb{Z}_p[x]$

Sean dos polinomios $p(x), q(x) \in \mathbb{Z}_p[x]$ *con* $q(x)$ *no nulo y p un número primo. Entonces existen dos únicos polinomios* $c(x), r(x) \in \mathbb{Z}_p[x]$, *llamados respectivamente cociente y resto de la división entre* $p(x)$ *y* $q(x)$, *que verifican:*

1) $p(x) = c(x).\, q(x) + r(x)$

2) $r(x) = 0 \ \vee \ grado(r(x)) < grado(q(x))$

Demostración

Véase [9], teniendo en cuenta que $\mathbb{Z}_p$ es un cuerpo pues *p* es un número primo. ■

Definición 5.2: Parte real y parte imaginaria de un octonión

Sea $o = \sum_{i=0}^{7} a_i \ e_i$ *un octonión y* $\overline{o}$ *su conjugado. Entonces*

1) La parte real de o es $Re(o) = \frac{(o + \overline{o})}{2}$. *Es decir,* $Re(o) = a_0$

2) La parte imaginaria de o es $Im(o) = \frac{(o - \overline{o})}{2}$. *Es decir,* $Im(o) = \sum_{i=1}^{7} a_i . e_i$

Proposición 5.3

Sea $o \in O$ un octonión. Entonces

$$o^2 = 2\,Re(o).\,o - |\,o\,|^2$$

Demostración

Como

$$Re(o) = \frac{(o+\bar{o})}{2}$$

Entonces

$$\bar{o} = 2\,Re(o) - o$$

Luego

$$|\,o\,|^2 = o\,.\,\bar{o} = o\,.(2\,Re(o) - o) = o\,.2\,Re(o) - o^2$$

Por lo tanto

$$|\,o\,|^2 = o\,.2\,Re(o) - o^2$$

De donde resulta

$$o^2 = 2\,Re(o).\,o - |\,o\,|^2 \qquad \blacksquare$$

Definición 5.4: Octoniones a coeficientes en $\mathbb{Z}_p$

El conjunto de octoniones a coeficientes en $\mathbb{Z}_p$ es

$$O(\mathbb{Z}_p) = \left\{ o = \sum_{i=0}^{7} a_i.\,e_i \;/\; a_i \in \mathbb{Z}_p \quad \forall i = 0,1,...,7 \right\}$$

Proposición 5.5:

Sea p un número primo y $o \in O(\mathbb{Z}_p)$. Entonces

1) Existen $\alpha, \beta \in \mathbb{Z}_p$ tales que

$$o^2 + \alpha.\,o + \beta = 0 \qquad en\ \mathbb{Z}_p$$

2) Dado un polinomio no constante $g(x) \in \mathbb{Z}_p[x]$, existen $a,b \in \mathbb{Z}_p$ tales que

$$g(o) = a.\,o + b \qquad en\ \mathbb{Z}_p$$

Demostración

1) Por la Proposición *5.3*, resulta

$$o^2 = 2\,Re(o).\,o - |\,o\,|^2$$

Luego

$$o^2 - 2\,Re(o).\,o + |\,o\,|^2 = 0$$

Tomando

α : *Resto de la división entera de* $-2\,Re(o)$ *por p.*

β : *Resto de la división entera de* $|\,o\,|^2$ *por p.*

Entonces, por la Proposición *2.4*, obtenemos

$$o^2 + \alpha.\,o + \beta \equiv 0 \quad (mod\ p)$$

Es decir

$$o^2 + \alpha.\,o + \beta = 0 \quad en\ \mathbb{Z}_p$$

2) Por el Teorema *5.1*, dado $g(x) \in \mathbb{Z}_p[x]$ y $q(x) = x^2 + \alpha\,x + \beta$, existen $c(x), r(x) \in \mathbb{Z}_p[x]$ tales que

$$g(x) = c(x).\,\left(x^2 + \alpha\,x + \beta\right) + r(x)$$

Donde

$$r(x) = 0 \ \vee\ grado\left(r(x)\right) < grado\left(q(x)\right)$$

Es decir,

$$r(x) = 0 \ \vee\ grado\left(r(x)\right) < 2$$

Por lo tanto

$$g(x) = c(x).\,\left(x^2 + \alpha\,x + \beta\right) + (a\,x + b)$$

Entonces, por el inciso 1) resulta

$$g(o) = c(o).\,\left(o^2 + \alpha\,o + \beta\right) + (a\,o + b) = c(o).\,0 + (a\,o + b) = a\,o + b \quad en\ \mathbb{Z}_p$$

Por lo tanto

$$g(o) = a\,o + b \quad en\ \mathbb{Z}_p \qquad \blacksquare$$

Proposición 5.6:

Sean los octoniones O_A, O_B, r_A *definidos en el Protocolo HK17. Entonces*

1) Existen $a,b,c,d \in \mathbb{Z}_p$ *tales que*

$$r_A = (a.\,O_A + b)\ O_B\ (c.\,O_A + d)$$

2) $(a.c,\ a.d,\ b.c,\ b.d)$ *es solución del sistema lineal*

$$r_A = (x_1, x_2, x_3, x_4)\ .\,A$$

Donde $A \in \mathbb{Z}_p^{4\times 8}$ *está definida por*

$$A = \begin{pmatrix} O_A.\,O_B.\,O_A \\ O_A.\,O_B \\ O_B.\,O_A \\ O_B \end{pmatrix}$$

Demostración

1) Por la Proposición *5.5* inciso *2*) existen $a,b,c,d \in \mathbb{Z}_p$ tales que

$$f(O_A)^m = a.\,O_A + b$$

$$f(O_A)^n = c.\,O_A + d$$

Por lo tanto

$$r_A = f(O_A)^m .\, O_B \;.\, f(O_A)^n = (a.\,O_A + b)\; O_B \;\; (c.\,O_A + d)$$

2) Por el inciso 1), al aplicar la propiedad distributiva del producto respecto de la suma, resulta

$$r_A = (a.\,O_A + b)\; O_B \;\; (c.\,O_A + d) = a.\,c\;.O_A.\,O_B.\,O_A + a.\,d\;.O_A.\,O_B + b.\,c\;.O_B.\,O_A + b.\,d\;.\,O_B =$$

$$= (a.c,\; a.d,\; b.c,\; b.d)\;.\begin{pmatrix} O_A.\,O_B.\,O_A \\ O_A.\,O_B \\ O_B.\,O_A \\ O_B \end{pmatrix} = (a.c,\; a.d,\; b.c,\; b.d)\;.A$$

En consecuencia, $(a.c,\; a.d,\; b.c,\; b.d)$ es solución del sistema lineal

$$r_A = (x_1, x_2, x_3, x_4)\;.A \qquad \blacksquare$$

Cómo hallar las constantes a, b, c , d $\in \mathbb{Z}_p$ que indica la Proposición 5.6

De acuerdo al inciso *2*) de la Proposición *5.6,* el sistema lineal no homogéneo en las incógnitas $x_1, x_2, x_3, x_4 \in \mathbb{Z}_p$, definido por

$$r_A = (x_1, x_2, x_3, x_4)\;.A \qquad [\text{ I }]$$

Tiene al menos una solución que es $(a.c,\; a.d,\; b.c,\; b.d)$. Además, sabemos que cualquier solución de este sistema es de la forma

$$(x_1, x_2, x_3, x_4) = (s_1, s_2, s_3, s_4) + (t_1, t_2, t_3, t_4)$$

Donde

(s_1, s_2, s_3, s_4): *Es una solución particular del sistema* [I].

(t_1, t_2, t_3, t_4): *Es una solución del sistema homogéneo* $0 = (x_1, x_2, x_3, x_4)\;.A$.

Por otro lado, también sabemos que la dimensión del espacio solución es

$$n - rango(A)$$

Donde

n: *Número de incógnitas del sistema. Es decir, n=4.*

$rango(A)$: *Rango de la matriz A*.

Teniendo en cuenta esta información, ¿cómo podemos obtener las constantes $a,b,c,d \in \mathbb{Z}_p$ a partir de una solución del sistema $r_A = (x_1, x_2, x_3, x_4)\ .\ A$?

Para responder a esta pregunta consideraremos dos casos:

Primer Caso: $rango(A) = 4$

En este caso, existe una única solución del sistema, ya que la dimensión del espacio solución es

$$n - rango(A) = 4 - 4 = 0$$

Sea (s_1, s_2, s_3, s_4) la única solución del sistema. Entonces, como $(a.c,\ a.d,\ b.c,\ b.d)$ es también solución, resulta

$$(s_1, s_2, s_3, s_4) = (a.c,\ a.d,\ b.c,\ b.d)$$

Por lo tanto, queda planteado el sistema:

$$\begin{cases} s_1 = a.c \\ s_2 = a.d \\ s_3 = b.c \\ s_4 = b.d \end{cases} \qquad \text{[II]}$$

Analizamos las siguientes situaciones:

1) Si $s_1 \neq 0$

En este caso, $a \neq 0 \ \wedge\ c \neq 0$. Entonces, de las tres primeras ecuaciones del sistema [II] obtenemos que

$$(a,\ b,\ c,\ d) = \left(a\ ,a\ s_1^{-1}s_3,\ a^{-1}s_1, a^{-1}s_2\right)$$

Observemos que esta igualdad es válida cualquier $a \neq 0$ en $\mathbb{Z}_p$. En particular, si tomamos $a = 1$ resulta

$$(a,\ b,\ c,\ d) = \left(1, s_1^{-1}s_3, s_1, s_2\right)$$

2) Si $s_1 = 0$

Entonces $a = 0 \ \vee\ c = 0$. De aquí concluimos que $s_2 = 0 \ \vee\ s_3 = 0$. Por lo tanto, analizamos las siguientes situaciones:

2.1) Si $s_2 = 0$, tomando $b = 1$ y reemplazando en el sistema [II] resulta

$$(a,\ b,\ c,\ d) = (0, 1, s_3, s_4)$$

2.2) Si $s_3 = 0$, tomando $d = 1$ y sustituyendo en el sistema [II] obtenemos

$$(a,\ b,\ c,\ d) = (s_2, s_4, 0, 1)$$

En cualquiera de estos casos, se verifica que

$$(a.O_A + b)\ O_B\ (c.O_A + d) = (s_1, s_2, s_3, s_4)\ .\ A = r_A$$

Segundo Caso: $rango(A) < 4$

En este caso, la dimensión del espacio solución es

$$n - rango(A) \geq 4 - 3 = 1$$

Luego, existe al menos una solución no trivial del sistema homogéneo asociado.

Por otro lado, sea (s_1, s_2, s_3, s_4) una solución particular del sistema [I]. Observemos que si algún a,b,c,d es cero, al menos dos de los valores $a.c, a.d, b.c, b.d$ son nulos. De este modo, y a fin de aplicar el Primer Caso, trataremos de hallar una solución (s'_1, s'_2, s'_3, s'_4) del sistema [I] tal que

$$s'_i \neq 0 \ \ \forall i=1,2,3,4 \quad \vee \quad card(\{ \ i \ tal \ que \ s'_i = 0\}) \geq 2 \qquad [III]$$

Donde

$card(B)$: *Cantidad de elementos que tiene un conjunto B.*

Para ello analizamos las siguientes situaciones:

1) (s_1, s_2, s_3, s_4) verifica las condiciones [III].

En este caso tomamos

$$(s'_1, s'_2, s'_3, s'_4) = (s_1, s_2, s_3, s_4)$$

2) (s_1, s_2, s_3, s_4) no verifica las condiciones [III].

En este caso,

$$\exists \ i_0 \ tal \ que \ s_{i_0} = 0 \quad \wedge \quad card(\{ \ i \ tal \ que \ s_i = 0\}) < 2$$

Es decir,

$$\exists \ i_0 \ tal \ que \ s_{i_0} = 0 \quad \wedge \quad card(\{ \ i \ tal \ que \ s_i = 0\}) \leq 1$$

Luego, existe exactamente un i_0 tal que $s_{i_0} = 0$. Sin pérdida de generalidad, podemos suponer que $i_0 = 1$. Por lo tanto

$$s_1 = 0 \quad \wedge \quad s_2, s_3, s_4 \neq 0$$

Consideremos ahora una solución no trivial (t_1, t_2, t_3, t_4) del sistema homogéneo

$$0 = (x_1, x_2, x_3, x_4) \ . A$$

2.1) Si $t_1 = 0$,

Entonces $t_2 \neq 0 \ \vee \ t_3 \neq 0 \ \vee t_4 \neq 0$. Sin pérdida de generalidad, supondremos que

$$t_2 \neq 0.$$

Calculamos $r = - s_2 \ . t_2^{-1} \in \mathbb{Z}_p$. Luego, tomamos

$$(s'_1, s'_2, s'_3, s'_4) = (s_1 + r.\, t_1,\ s_2 + r.\, t_2,\ s_3 + r.\, t_3,\ s_4 + r.\, t_4) = (0,\ 0,\ s_3 + r.\, t_3,\ s_4 + r.\, t_4)$$

Es decir,

$$(s'_1, s'_2, s'_3, s'_4) = (0,\ 0,\ s_3 + r.\, t_3,\ s_4 + r.\, t_4)$$

2.2) Si $t_1 \neq 0$,

Buscamos un $r \in \mathbb{Z}_p$ de modo tal que

$$s_i + r.\, t_i \neq 0 \quad en\ \mathbb{Z}_p,\ \forall i=1,2,3,4.$$

Dicho *r* puede ser hallado ya que el número primo *p* es suficientemente grande.
Luego, tomamos

$$(s'_1,s'_2,s'_3,s'_4) = (s_1 + r.\, t_1,\ s_2 + r.\, t_2,\ s_3 + r.\, t_3,\ s_4 + r.\, t_4) = (r.\, t_1,\ s_2 + r.\, t_2,\ s_3 + r.\, t_3,\ s_4 + r.\, t_4)$$

Es decir,

$$(s'_1,s'_2,s'_3,s'_4) = (r.\, t_1,\ s_2 + r.\, t_2,\ s_3 + r.\, t_3,\ s_4 + r.\, t_4)$$

De este modo, en ambos casos, podemos encontrar una solución (s'_1,s'_2,s'_3,s'_4) tal que $s'_i \neq 0\ \ \forall i=1,2,3,4$ o que al menos dos de los s'_i sean nulos. Luego aplicamos el Primer Caso a la solución (s'_1,s'_2,s'_3,s'_4) para calcular $(a,\ b,\ c,\ d)$.

El siguiente Ejemplo ayudará a comprender cómo hallar $(a,\ b,\ c,\ d)$ a partir de este procedimiento.

Ejemplo 5.7

En el protocolo HK17, consideremos:

$p=11$

$O_A = (1,0,2,5,0,2,7,10)$

$O_B = (0,0,3,8,1,0,4,2)$

$m=3$, $n=5$, $f(x) = 4x^3 + 11x$

1) Calcular $r_A = [\, f(O_A)]^m . O_B\ .[\, f(O_A)]^n$

2) Hallar *a, b, c, d* de modo tal que $r_A = (a.\, O_A + b).\, O_B\ .(c.\, O_A + d)$

Solución

1) Teniendo en cuenta que las operaciones entre octoniones se realizan en $\mathbb{Z}_p$, y considerando la suma y producto de octoniones definidos en el Capítulo *3*, resulta:

$$r_A = [\, f(O_A)]^m . O_B\ .[\, f(O_A)]^n = (2,2,6,3,8,3,5,3)$$

2) Para hallar *a, b, c, d* resolvemos primeramente el sistema

$$r_A = (x_1,x_2,x_3,x_4)\ .\ A$$

Donde

$$A = \begin{pmatrix} O_A.\, O_B.\, O_A \\ O_A.\, O_B \\ O_B.\, O_A \\ O_B \end{pmatrix} = \begin{pmatrix} 10 & 0 & 8 & 7 & 7 & 9 & 10 & 4 \\ 5 & 6 & 5 & 7 & 8 & 0 & 2 & 9 \\ 5 & 5 & 1 & 9 & 5 & 0 & 6 & 6 \\ 0 & 0 & 3 & 8 & 1 & 0 & 4 & 2 \end{pmatrix}$$

Este sistema es equivalente a transponerlo miembro a miembro:

$$r_A^T = \left[\left(x_1, x_2, x_3, x_4 \right) . A \right]^T$$

Es decir

$$r_A^T = A^T . \left(x_1, x_2, x_3, x_4 \right)^T$$

De donde resulta

$$\begin{pmatrix} 10 & 5 & 5 & 0 \\ 0 & 6 & 5 & 0 \\ 8 & 5 & 1 & 3 \\ 7 & 7 & 9 & 8 \\ 7 & 8 & 5 & 1 \\ 9 & 0 & 0 & 0 \\ 10 & 2 & 6 & 4 \\ 4 & 9 & 6 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 6 \\ 3 \\ 8 \\ 3 \\ 5 \\ 3 \end{pmatrix}$$

Para resolver este sistema, aplicaremos el Método de Eliminación de Gauss, teniendo en cuenta que las operaciones se llevan a cabo en $\mathbb{Z}_{11}$. Para ello triangularemos la matriz ampliada asociada al sistema:

$$\left(\begin{array}{cccc|c} 10 & 5 & 5 & 0 & 2 \\ 0 & 6 & 5 & 0 & 2 \\ 8 & 5 & 1 & 3 & 6 \\ 7 & 7 & 9 & 8 & 3 \\ 7 & 8 & 5 & 1 & 8 \\ 9 & 0 & 0 & 0 & 3 \\ 10 & 2 & 6 & 4 & 5 \\ 4 & 9 & 6 & 2 & 3 \end{array}\right) \xrightarrow{\textit{Primer Paso}} \left(\begin{array}{cccc|c} 1 & 6 & 6 & 0 & 9 \\ 0 & 6 & 5 & 0 & 2 \\ 0 & 1 & 8 & 3 & 0 \\ 0 & 9 & 0 & 8 & 6 \\ 0 & 10 & 7 & 1 & 0 \\ 0 & 1 & 1 & 0 & 10 \\ 0 & 8 & 1 & 4 & 3 \\ 0 & 7 & 4 & 2 & 0 \end{array}\right) \xrightarrow{\textit{Segundo Paso}}$$

$$\left(\begin{array}{cccc|c} 1 & 6 & 6 & 0 & 9 \\ 0 & 1 & 10 & 0 & 4 \\ 0 & 0 & 9 & 3 & 7 \\ 0 & 0 & 9 & 8 & 3 \\ 0 & 0 & 6 & 1 & 4 \\ 0 & 0 & 2 & 0 & 6 \\ 0 & 0 & 9 & 4 & 4 \\ 0 & 0 & 0 & 2 & 0 \end{array}\right) \xrightarrow{\textit{Tercer Paso}} \left(\begin{array}{cccc|c} 1 & 6 & 6 & 0 & 9 \\ 0 & 1 & 10 & 0 & 4 \\ 0 & 0 & 1 & 4 & 2 \\ 0 & 0 & 0 & 5 & 7 \\ 0 & 0 & 0 & 10 & 3 \\ 0 & 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 & 8 \\ 0 & 0 & 0 & 2 & 5 \end{array}\right) \xrightarrow{\textit{Cuarto Paso}}$$

$$\left(\begin{array}{cccc|c} 1 & 6 & 6 & 0 & 9 \\ 0 & 1 & 10 & 0 & 4 \\ 0 & 0 & 1 & 4 & 2 \\ 0 & 0 & 0 & 1 & 8 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Los detalles de cada paso efectuado hasta triangular la matriz los expondremos a continuación, teniendo en cuenta que utilizaremos la Proposición *2.14* para calcular el inverso de un elemento no nulo en $\mathbb{Z}_p$. Además, aplicaremos la siguiente propiedad:

$$a \equiv a + k.p \pmod{p} \quad \forall a\,,\, k \in \mathbb{Z}\,.$$

Por otro lado, llamaremos F_i a la *i*-ésima fila de la matriz ampliada.

Primer Paso:

$$F_1 := 10^{-1}.F_1 = 10.F_1 = (100,50,50,0,20) \equiv (1,6,6,0,9)$$

$$F_3 := F_3 - 8.F_1 = (8,5,1,3,6) - 8.(1,6,6,0,9) = (0,-43,-47,3,-66) \equiv$$
$$\equiv (0,-43+4\times 11,-47+5\times 11,3,-66) = (0,1,8,3,0)$$

$$F_4 := F_4 - 7.F_1 = (7,7,9,8,3) - 7.(1,6,6,0,9) = (0,-35,-33,8,-60) \equiv$$
$$\equiv (0,-35+4\times 11,-33+3\times 11,8,-60+6\times 11) = (0,9,0,8,6)$$

$$F_5 := F_5 - 7.F_1 = (7,8,5,1,8) - 7.(1,6,6,0,9) = (0,-34,-37,1,-55) \equiv$$
$$\equiv (0,-34+4\times 11,-37+4\times 11,1,-55+5\times 11) = (0,10,7,1,0)$$

$$F_6 := F_6 - 9.F_1 = (9,0,0,0,3) - 9.(1,6,6,0,9) = (0,-54,-54,0,-78) \equiv$$
$$\equiv (0,-54+5\times 11,-54+5\times 11,0,-78+8\times 11) = (0,1,1,0,10)$$

$$F_7 := F_7 - 10.F_1 = (10,2,6,4,5) - 10.(1,6,6,0,9) = (0,-58,-54,4,-85) \equiv$$
$$\equiv (0,-58+6\times 11,-54+5\times 11,4,-85+8\times 11) = (0,8,1,4,3)$$

$$F_8 := F_8 - 4.F_1 = (4,9,6,2,3) - 4.(1,6,6,0,9) = (0,-15,-18,2,-33) \equiv$$
$$\equiv (0,-15+2\times 11,-18+2\times 11,2,-33+3\times 11) = (0,7,4,2,0)$$

Segundo Paso:

$$F_2 := 6^{-1}.F_2 = 2.F_2 = 2.(0,6,5,0,2) = (0,12,10,0,4) \equiv (0,1,10,0,4)$$

$$F_3 := F_3 - 1.F_2 = (0,1,8,3,0) - (0,1,10,0,4) = (0,0,-2,3,-4) \equiv$$
$$\equiv (0,0,-2+11,3,-4+11) = (0,0,9,3,7)$$

$$F_4 := F_4 - 9.F_2 = (0,9,0,8,6) - 9.(0,1,10,0,4) = (0,0,-90,8,-30) \equiv$$

$$\equiv (0,0,-90+9\times 11,8,-30+3\times 11) = (0,0,9,8,3)$$

$$F_5 := F_5 - 10.F_2 = (0,10,7,1,0) - 10.(0,1,10,0,4) = (0,0,-93,1,-40) \equiv$$
$$\equiv (0,0,-93+9\times 11,1,-40+4\times 11) = (0,0,6,1,4)$$

$$F_6 := F_6 - 1.F_2 = (0,1,1,0,10) - (0,1,10,0,4) = (0,0,-9,0,6) \equiv$$
$$\equiv (0,0,-9+11,0,6) = (0,0,2,0,6)$$

$$F_7 := F_7 - 8.F_2 = (0,8,1,4,3) - 8.(0,1,10,0,4) = (0,0,-79,4,-29) \equiv$$
$$= (0,0,-79+8\times 11,4,-29+3\times 11) = (0,0,9,4,4)$$

$$F_8 := F_8 - 7.F_2 = (0,7,4,2,0) - 7.(0,1,10,0,4) = (0,0,-66,2,-28) \equiv$$
$$\equiv (0,0,-66+6\times 11,2,-28+3\times 11) = (0,0,0,2,5)$$

Tercer Paso:

$$F_3 := 9^{-1}.F_3 = 5.F_3 = 5.(0,0,9,3,7) = (0,0,45,15,35) \equiv (0,0,1,4,2)$$

$$F_4 := F_4 - 9.F_3 = (0,0,9,8,3) - 9.(0,0,1,4,2) = (0,0,0,-28,-15) \equiv$$
$$\equiv (0,0,0,-28+3\times 11,-15+2\times 11) = (0,0,0,5,7)$$

$$F_5 := F_5 - 6.F_3 = (0,0,6,1,4) - 6.(0,0,1,4,2) = (0,0,0,-23,-8) \equiv$$
$$\equiv (0,0,0,-23+3\times 11,-8+11) = (0,0,0,10,3)$$

$$F_6 := F_6 - 2.F_3 = (0,0,2,0,6) - 2.(0,0,1,4,2) = (0,0,0,-8,2) \equiv$$
$$\equiv (0,0,0,-8+11,2) = (0,0,0,3,2)$$

$$F_7 := F_7 - 9.F_3 = (0,0,9,4,4) - 9.(0,0,1,4,2) = (0,0,0,-32,-14) \equiv$$
$$\equiv (0,0,0,-32+3\times 11,-14+2\times 22) = (0,0,0,1,8)$$

Cuarto Paso:

$$F_4 := 5^{-1}.F_4 = 9.F_4 = 9.(0,0,0,5,7) = (0,0,0,45,63) \equiv (0,0,0,1,8)$$

$$F_5 := F_5 - 10.F_4 = (0,0,0,10,3) - 10.(0,0,0,1,8) = (0,0,0,0,-77) \equiv$$
$$\equiv (0,0,0,0,-77+7\times 11) = (0,0,0,0,0)$$

$$F_6 := F_6 - 3.F_4 = (0,0,0,3,2) - 3.(0,0,0,1,8) = (0,0,0,0,-22) \equiv$$
$$\equiv (0,0,0,0,-22+2\times 11) = (0,0,0,0,0)$$

$$F_7 := F_7 - 31.F_4 = (0,0,0,1,8) - (0,0,0,1,8) = (0,0,0,0,0)$$

$$F_8 := F_8 - 2.F_4 = (0,0,0,2,5) - 2(0,0,0,1,8) = (0,0,0,0,-11) \equiv$$
$$\equiv (0,0,0,0,-11+11) = (0,0,0,0,0)$$

Podemos comprobar que $rango(A)=4$, ya que el número de filas no nulas de la matriz triangulada es *4*. Por lo tanto, el sistema tiene una única solución, que la llamaremos

$$(s_1,s_2,s_3,s_4)$$

Para hallar la solución, expresamos la matriz triangulada en términos de las ecuaciones asociadas:

$$\begin{cases} s_1+6\ s_2+6\ s_3 = 9 \\ s_2+10s_3 = 4 \\ s_3+4s_4 = 2 \\ s_4 = 8 \end{cases}$$

De la cuarta ecuación obtenemos

$$s_4 = 8$$

Reemplazando s_4 en la tercera ecuación resulta

$$s_3+4\times 8=2$$

Entonces

$$s_3 = 2-32 = -30 \equiv -30+3\times 11 = 3$$

Luego

$$s_3 = 3$$

Sustituyendo s_3 en la segunda ecuación obtenemos

$$s_2+10\times 3 = 4$$

Por lo tanto

$$s_2 = 4-30 = -26 \equiv -26+3\times 11 = 7$$

Es decir

$$s_2 = 7$$

Finalmente, reemplazando s_2 y s_3 en la primera ecuación resulta

$$s_1+6\times 7+6\times 3 = 9$$

Entonces

$$s_1 = 9-42-18 = -51 \equiv -51+5\times 11 = 4$$

En consecuencia, la solución es

$$(s_1,s_2,s_3,s_4)=(4,7,3,8)$$

Como $s_1 \neq 0$, tomamos

$$(a,b,c,d)=\left(1,s_1^{-1}.\ s_3,s_1,s_2\right)=\left(1,4^{-1}\times 3,4,7\right)=(1,3\times 3,4,7)=(1,9,4,7)$$

Es decir

$$(a,b,c,d)=(1,9,4,7)$$

Se puede comprobar que efectivamente $(a.\ O_A+b).\ O_B\ .(c.\ O_A+d)=r_A$ pues

$$(a.\ O_A+b).\ O_B\ .(c.\ O_A+d)=(1.\ O_A+9).\ O_B\ .(4.\ O_A+7)=$$
$$=(10,0,2,5,0,2,7,10).(0,0,3,8,1,0,4,2).(11,0,8,20,0,8,28,40)=$$
$$=(5,6,10,2,6,0,5,5).(11,0,8,20,0,8,28,40)=(2,2,6,3,8,3,5,3)=r_A.$$

El Método de Eliminación de Gauss en $\mathbb{Z}_p$ aplicando Mathematica

El siguiente programa, diseñado mediante el software Wolfram Mathematica *11.0*, aplica el Método de Eliminación de Gauss a fin de triangular una matriz *A* de *8* filas y *5* columnas con coeficientes en $\mathbb{Z}_p$, donde *p* es un número primo:

```
p = 11;
A = {{10, 5, 5, 0, 2}, {0, 6, 5, 0, 2}, {8, 5, 1, 3, 6}, {7, 7, 9, 8, 3}, {7, 8, 5, 1, 8},
  {9, 0, 0, 0, 3}, {10, 2, 6, 4, 5}, {4, 9, 6, 2, 3}};
For[i = 1, i ≤ 4, i++,
 If[A[[i, i]] == 0,
  (*Si A[[i,i]]=0, intercambio la k-ésima fila con la i-ésima*)
  Encontrado = 0;
  k = i + 1;
  While[Encontrado == 0 && k ≤ 8,
   If[A[[k, i]] ≠ 0,
    Encontrado = 1;
    Aux = A[[i]];
    A[[i]] = A[[k]];
    A[[k]] = Aux,
    k++;
   ]
  ]
 ];
 If[A[[i, i]] ≠ 0,
  (*Calculamos el inverso de A[[i,i]] en Zp*)
  Encontrado = 0;
  k = 1;
 While[k ≤ A[[i, i]] && Encontrado == 0,
  If[Mod[1 + p * k, A[[i, i]]] == 0, Encontrado = 1];
  k++;
 ];
 inv = (1 + p * (k - 1))/A[[i, i]];
 (*Multiplicamos la i-ésima fila por el inverso de A[[i,i]] en Zp*)
 A[[i]] = Mod[inv * A[[i]], p];
 For[j = i + 1, j ≤ 8, j++,
  A[[j]] = Mod[A[[j]] - A[[j, i]] * A[[i]], p]

 ];
 ]
]
Print["La matriz triangulada es:", MatrixForm[A]]
```

Antes de describir el algoritmo de ataque del protocolo HK17, enunciaremos la siguiente Proposición:

Proposición 5.8:

En el Protocolo HK17, si dos polinomios $g_1(x), g_2(x) \in \mathbb{Z}_p[x]$ *son tales que*

$$r_A = g_1(O_A).\, O_B.\, g_2(O_A)$$

Entonces la clave que comparten Alicia y Bernardo es

$$K = g_1(O_A).\, r_B.\, g_2(O_A)$$

Demostración

Sea K_B la clave generada por Bernardo. Entonces, aplicando las Proposiciones *2.58* y *2.59* resulta

$$K = K_B = \left[h(O_A)\right]^r . r_A .\, \left[h(O_A)\right]^s = \left[h(O_A)\right]^r .\, \left(g_1(O_A).\, O_B.\, g_2(O_A)\right).\, \left[h(O_A)\right]^s =$$

$$= \left(\left[h(O_A)\right]^r . g_1(O_A)\right).\, O_B.\, \left(g_2(O_A).\left[h(O_A)\right]^s\right) =$$

$$\left(g_1(O_A).\left[h(O_A)\right]^r\right).\, O_B.\, \left(\left[h(O_A)\right]^s . g_2(O_A)\right) = g_1(O_A).\left(\left[h(O_A)\right]^r .O_B.\left[h(O_A)\right]^s\right).\, g_2(O_A) =$$

$$= g_1(O_A).\, r_B.\, g_2(O_A) \qquad \blacksquare$$

Finalmente, enunciaremos a continuación el algoritmo de ataque.

Algoritmo de ataque al Protocolo de HK17

<u>*Primer Paso*</u>

Una vez capturados los octoniones O_A, O_B , r_A *y* r_B *, calcular a, b, c, d de modo tal que*

$$r_A = (a.\, O_A + b)\; O_B\; (c.\, O_A + d)$$

Esto es posible en virtud de la Proposición 5.6.

<u>*Segundo Paso*</u>

La clave que comparten Alicia y Bernardo es

$$K = (a.\, O_A + b).\, r_B.\, (c.\, O_A + d)$$

En el siguiente Ejemplo verificaremos el funcionamiento de este algoritmo.

Ejemplo 5.9

En el Ejemplo *4.2*, un intruso observa la información que intercambian Alicia y Bernardo, y captura los siguientes datos:

$p=13$

$O_A=(1,\ 2,\ 10,\ 0,\ 0,\ 5,\ 11,\ 0)$

$O_B=(3,\ 0,\ 9,\ 1,\ 0,\ 1,\ 0,\ 0)$

$r_A=(11,\ 1\ ,9\ ,9\ ,2\ ,11\ ,6\ ,\ 9)$

$r_B=(11,2,0,9,0,1,11,0)$

Aplicar el algoritmo de ataque al HK17 para descubrir la clave que comparten Alicia y Bernardo.

Solución

Primer Paso

Calculamos *a, b, c, d*, de modo tal que

$$r_A=(a.\ O_A+b)\ O_B\ (c.\ O_A+d)$$

Para ello resolvemos primeramente el sistema

$$r_A=(x_1,x_2,x_3,x_4)\ .\ A$$

Donde

$$A=\begin{pmatrix} O_A.O_B.O_A \\ O_A.O_B \\ O_B.O_A \\ O_B \end{pmatrix}=\begin{pmatrix} 12 & 9 & 3 & 4 & 0 & 7 & 4 & 0 \\ 12 & 8 & 8 & 10 & 3 & 0 & 9 & 7 \\ 12 & 4 & 5 & 5 & 10 & 6 & 5 & 6 \\ 3 & 0 & 9 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Este sistema es equivalente a

$$r_A^T=A^T.(x_1,x_2,x_3,x_4)^T$$

Es decir

$$\begin{pmatrix} 12 & 12 & 12 & 3 \\ 9 & 8 & 4 & 0 \\ 3 & 8 & 5 & 9 \\ 4 & 10 & 5 & 1 \\ 0 & 3 & 10 & 0 \\ 7 & 0 & 6 & 1 \\ 4 & 9 & 5 & 0 \\ 0 & 7 & 6 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}=\begin{pmatrix} 11 \\ 1 \\ 9 \\ 9 \\ 2 \\ 11 \\ 6 \\ 9 \end{pmatrix}$$

Para resolverlo, utilizaremos el programa que diseñamos con el software Wolfram Mathematica *11.0*, a fin de triangular la matriz ampliada del sistema:

$$\left(\begin{array}{cccc|c} 12 & 12 & 12 & 3 & 11 \\ 9 & 8 & 4 & 0 & 1 \\ 3 & 8 & 5 & 9 & 9 \\ 4 & 10 & 5 & 1 & 9 \\ 0 & 3 & 10 & 0 & 2 \\ 7 & 0 & 6 & 1 & 11 \\ 4 & 9 & 5 & 0 & 6 \\ 0 & 7 & 6 & 0 & 9 \end{array}\right)$$

Al ejecutar el programa, obtenemos la siguiente matriz:

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 10 & 2 \\ 0 & 1 & 5 & 12 & 4 \\ 0 & 0 & 1 & 12 & 3 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vemos que $rango(A)=4$, ya que el número de filas no nulas de la matriz triangulada es *4*. Por lo tanto, el sistema tiene una única solución, que la llamaremos

$$(s_1,s_2,s_3,s_4)$$

Para hallar la solución, expresamos la matriz triangulada en términos de las ecuaciones asociadas:

$$\begin{cases} s_1+s_2+\ \ s_3+10s_4=2 \\ \quad\ s_2+5s_3\ +12s_4=4 \\ \quad\quad\ \ s_3\ +12s_4=3 \\ \quad\quad\quad\quad\ \ s_4=4 \end{cases}$$

Al resolver este sistema, y teniendo en cuenta que las operaciones se efectúan en $\mathbb{Z}_{13}$, obtenemos

$$(s_1,s_2,s_3,s_4)=(8,12,7,4)$$

Como $s_1\neq 0$, tomamos

$$(a,b,c,d)=\left(1,s_1^{-1}.\ s_3,s_1,s_2\right)=\left(1,8^{-1}\times 7,8,12\right)=(1,5\times 7,8,12)=(1,35,8,12)\equiv(1,9,8,12)$$

Es decir

$$(a,b,c,d)=(1,9,8,12)$$

Segundo Paso

Calculamos

$$K=(a.\,O_A+b)\ r_B\ (c.\,O_A+d)=(1.\,O_A+9)\ r_B\ (8.\,O_A+12)=$$
$$=(10,2,10,0,0,5,11,0)\ .(11,2,0,9,0,1,11,0).\ (20,16,80,0,0,40,88,0)\equiv$$
$$=(10,2,10,0,0,5,11,0)\ .(11,2,0,9,0,1,11,0).\ (7,3,2,0,0,1,10,0)=$$
$$=(6,8,0,2,1,12,2,11).\ (7,3,2,0,0,1,10,0)=(12,8,11,3,5,12,3,3)$$

Por lo tanto,

$$K=(12,8,11,3,5,12,3,3)$$

Al analizar el Ejemplo *4.2,* que aplica el Protocolo HK17, corroboramos que *K* es efectivamente la clave que comparten Alicia y Bernardo.

A continuación enunciaremos el Ejemplo de Protocolo HK17 propuesto en [4], para luego atacarlo y descubrir su clave. Primeramente desarrollaremos dicho Ejemplo.

Ejemplo 5.10

Alicia y Bernardo decidieron aplicar el Protocolo HK17 a fin de generar una clave que compartirán. Para ello se ejecutan los siguientes pasos:

Primer Paso

Alicia elige como elementos públicos a dos octoniones O_A y O_B a coeficientes en $\mathbb{Z}_p$, considerando $p=251$:

$$O_A=(157,188,177,188,203,149,217,148)$$
$$O_B=(40,207,6,33,75,79,98,54)$$

Segundo Paso

Alicia elige como clave privada dos enteros $m=4$, $n=122$ y el polinomio

$$f(x)=97x^{15}+98x^{14}+6x^{13}+136x^{12}+238x^{11}+150x^{10}+5x^9+135x^8+186x^7+83x^6+168x^5+$$
$$+90x^4+238x^3+249x^2+150x+180\ .$$

Luego envía a Bernardo O_A y O_B por un canal inseguro.

Tercer Paso

Bernardo elige como clave privada dos enteros $r=17$, $s=177$ y el polinomio

$$h(x)=157x^{15}+48x^{14}+53x^{13}+124x^{12}+76x^{11}+33x^{10}+166x^9+76x^8+150x^7+52x^6+50x^5+$$
$$+40x^4+114x^3+58x^2+97x+5$$

Cuarto Paso

Alicia calcula

$$r_A = \left[f\left(O_A\right)\right]^m . O_B . \left[f\left(O_A\right)\right]^n$$

Obteniendo por resultado

$$r_A = \left(121,3,110,243,184,230,202,171\right)$$

Alicia envía este octonión a Bernardo. Por otro lado, Bernardo calcula

$$r_B = \left[h\left(O_A\right)\right]^r . O_B . \left[h\left(O_A\right)\right]^s$$

Y obtiene

$$r_B = \left(90,42,17,119,150,23,110,182\right)$$

Quinto Paso

Alicia calcula su clave

$$K_A = \left[f\left(O_A\right)\right]^m . r_B . \left[f\left(O_A\right)\right]^n$$

Resultando

$$K_A = \left(84,242,130,31,84,244,45,20\right)$$

Por otro lado, Bernardo calcula su clave

$$K_B = \left[h\left(O_A\right)\right]^r . r_A . \left[h\left(O_A\right)\right]^s$$

Luego

$$K_B = \left(84,242,130,31,84,244,45,20\right)$$

Finalmente, Alicia y Bernardo comparten la clave

$$K = K_A = K_B = \left(84,242,130,31,84,244,45,20\right)$$

Ahora aplicaremos, al Ejemplo anterior, el algoritmo de ataque para descubrir su clave.

Ejemplo 5.11

En el Ejemplo anterior, teniendo en cuenta que

$p = 251$

$O_A = \left(157,188,177,188,203,149,217,148\right)$

$O_B = \left(40,207,6,33,75,79,98,54\right)$

$r_A = \left(121,3,110,243,184,230,202,171\right)$

$r_B = \left(90,42,17,119,150,23,110,182\right)$

Aplicar el algoritmo de ataque al Protocolo HK17 para hallar la clave K que Alicia y Bernardo comparten.

Solución

Primer Paso

Calculamos *a, b, c, d,* de modo tal que

$$r_A = (a.\,O_A + b)\;O_B\;(c.\,O_A + d)$$

Para ello resolvemos primeramente el sistema

$$r_A = (x_1, x_2, x_3, x_4)\;.\,A$$

Donde

$$A = \begin{pmatrix} O_A.\,O_B.\,O_A \\ O_A.\,O_B \\ O_B.\,O_A \\ O_B \end{pmatrix} = \begin{pmatrix} 83 & 15 & 112 & 103 & 214 & 85 & 170 & 210 \\ 228 & 85 & 171 & 121 & 97 & 11 & 29 & 82 \\ 228 & 135 & 60 & 181 & 35 & 69 & 162 & 100 \\ 40 & 207 & 6 & 33 & 75 & 79 & 98 & 54 \end{pmatrix}$$

Este sistema es equivalente a

$$r_A^T = A^T.(x_1, x_2, x_3, x_4)^T$$

Es decir

$$\begin{pmatrix} 83 & 228 & 228 & 40 \\ 15 & 85 & 135 & 207 \\ 112 & 171 & 60 & 6 \\ 103 & 121 & 181 & 33 \\ 214 & 97 & 35 & 75 \\ 85 & 11 & 69 & 79 \\ 170 & 29 & 162 & 98 \\ 210 & 82 & 100 & 54 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 121 \\ 3 \\ 110 \\ 243 \\ 184 \\ 230 \\ 202 \\ 171 \end{pmatrix}$$

Para resolverlo, utilizaremos el programa que diseñamos con el software Wolfram Mathematica *11.0*, a fin de triangular la matriz ampliada del sistema:

$$\left(\begin{array}{cccc|c} 83 & 228 & 228 & 40 & 121 \\ 15 & 85 & 135 & 207 & 3 \\ 112 & 171 & 60 & 6 & 110 \\ 103 & 121 & 181 & 33 & 243 \\ 214 & 97 & 35 & 75 & 184 \\ 85 & 11 & 69 & 79 & 230 \\ 170 & 29 & 162 & 98 & 202 \\ 210 & 82 & 100 & 54 & 171 \end{array}\right)$$

Al ejecutar el programa, obtenemos la siguiente matriz:

$$\left(\begin{array}{cccc|c} 1 & 160 & 160 & 191 & 195 \\ 0 & 1 & 27 & 164 & 97 \\ 0 & 0 & 1 & 118 & 247 \\ 0 & 0 & 0 & 1 & 199 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vemos que $rango(A)=4$, ya que el número de filas no nulas de la matriz triangulada es *4*. Por lo tanto, el sistema tiene una única solución, que la llamaremos

$$(s_1,s_2,s_3,s_4)$$

Para hallar la solución, expresamos la matriz triangulada en términos de las ecuaciones asociadas:

$$\begin{cases} s_1+160s_2+160\ \ s_3+191\ s_4=195 \\ \qquad\quad s_2+27\ \ \ s_3\ +164\ s_4=97 \\ \qquad\qquad\qquad\ \ s_3\ +118\ s_4=247 \\ \qquad\qquad\qquad\qquad\quad s_4=199 \end{cases}$$

Al resolver este sistema, y teniendo en cuenta que las operaciones se efectúan en $\mathbb{Z}_{251}$, obtenemos

$$(s_1,s_2,s_3,s_4)=(75,187,108,199)$$

Como $s_1\neq 0$, tomamos

$$(a,b,c,d)=\left(1,s_1^{-1}.\ s_3,s_1,s_2\right)=\left(1,(75)^{-1}\times 108,75,187\right)=(1,164\times 108,75,187)=$$

$$=(1,17712,75,187)\equiv(1,142,75,187)$$

Es decir

$$(a,b,c,d)=(1,142,75,187)$$

<u>*Segundo Paso*</u>

Calculamos

$$K=(a.\ O_A+b)\ r_B\ \ (c.\ O_A+d)=(1.\ O_A+142)\ r_B\ \ (75.\ O_A+187)=(84,242,130,31,84,244,45,20)$$

Por lo tanto,

$$K=(84,242,130,31,84,244,45,20)$$

Como podemos comprobar, es ésta la clave *K* que comparten Alicia y Bernardo.

2. Descifrado de la clave del Protocolo de Diffie-Hellman aplicando Cuaterniones.

Recordemos que un cuaternión ***q*** es una expresión de la forma

$$q = a + b\ i + c\ j + d\ k$$

Donde $a, b, c, d \in \mathbb{R}$ e i, j, k son unidades imaginarias que verifican las siguientes igualdades:

$$i^2 = j^2 = k^2 = i.j.k = -1$$

Además, el cuaternión puede representarse como un vector en $\mathbb{R}^4$, es decir,

$$q = (a,\ b\ ,c\ ,d\ )$$

Por otro lado, un octonión ***o*** es una expresión de la forma

$$o = \sum_{i=0}^{7} a_i\ e_i$$

Donde $a_i \in \mathbb{R}\ \forall\ i = 0, 1, ..., 7$, $e_1, e_2, ..., e_7$ son unidades imaginarias y $e_0 = 1$.

El octonión puede representarse mediante un vector en $\mathbb{R}^8$, del siguiente modo:

$$o = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$$

Recordemos también que cualquier cuaternión ***q*** puede representarse como un octonión. Es decir, dado el cuaternión

$$q = (a,b,c,d)$$

Entonces ***q*** es un octonión de la forma

$$q = (a,b,c,0,d,0,0,0)$$

Considerando $e_0 = 1$, $e_1 = i$, $e_2 = j$, $e_4 = k$, $a_3 = a_5 = a_6 = a_7 = 0$.

Así, las operaciones aritméticas entre cuaterniones pueden efectuarse en términos de octoniones. En base a este resultado, los Teoremas y Proposiciones mencionados en este Capítulo siguen siendo válidos para cuaterniones. Pero en lugar de operar en $\mathbb{Z}_p$ se opera en $\mathbb{R}$..

En consecuencia, el Algoritmo de ataque al Protocolo HK17 puede aplicarse al de Diffie-Hellman que emplea cuaterniones. En el siguiente Ejemplo mostraremos su modo de implementación.

Ejemplo 5.12

En el Ejemplo *4.2*, Alicia y Bernardo decidieron generar una clave de seguridad mediante el Algoritmo de Diffie-Hellman empleando cuaterniones. Un intruso capturó los siguientes cuaterniones:

$$q_A = \left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$$

$$q_B = \left(\frac{3}{5},0,\frac{4}{5},0\right)$$

$$r_A = (0,06145\ ,0,05370\ ,\ -0,4969\ ,\ -0,8640)$$

$$r_B = (0,5156\ ,-0,1976\ ,0,4680\ ,0,6899)$$

¿Podrá el intruso descubrir la clave que comparten Alicia y Bernardo?

Solución

Para hallar la clave, aplicaremos el Algoritmo de ataque al Protocolo HK17. Para ello expresaremos primeramente como octoniones a los cuaterniones q_A, q_B, r_A, r_B *:*

$$q_A = \left(\frac{1}{2},\frac{1}{2},\frac{1}{2},0,\frac{1}{2},0,0,0\right)$$

$$q_B = \left(\frac{3}{5},0,\frac{4}{5},0,0,0,0,0\right)$$

$$r_A = (0.06145,0.05370,-0.4969,0,-0.8640,0,0,0)$$

$$r_B = (0.5156,-0.1976,0.4680,0,0.6899,0,0,0)$$

<u>*Primer Paso*</u>

Calculamos *a, b, c, d,* de modo tal que

$$r_A = (a.\,O_A + b)\ O_B\ (c.\,O_A + d)$$

Para ello resolvemos el sistema

$$r_A = (x_1,x_2,x_3,x_4)\ .\ A$$

Donde

$$A = \begin{pmatrix} O_A.\,O_B.\,O_A \\ O_A.\,O_B \\ O_B.\,O_A \\ O_B \end{pmatrix} = \begin{pmatrix} -\frac{7}{10} & -\frac{1}{10} & \frac{7}{10} & 0 & -\frac{1}{10} & 0 & 0 & 0 \\ -\frac{1}{10} & -\frac{1}{10} & \frac{7}{10} & 0 & \frac{7}{10} & 0 & 0 & 0 \\ -\frac{1}{10} & \frac{7}{10} & \frac{7}{10} & 0 & -\frac{1}{10} & 0 & 0 & 0 \\ \frac{3}{5} & 0 & \frac{4}{5} & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Este sistema es equivalente a

$$r_A^T = A^T.(x_1,x_2,x_3,x_4)^T$$

Es decir

$$\begin{pmatrix} -\frac{7}{10} & -\frac{1}{10} & -\frac{1}{10} & \frac{3}{5} \\ -\frac{1}{10} & -\frac{1}{10} & \frac{7}{10} & 0 \\ \frac{7}{10} & \frac{7}{10} & \frac{7}{10} & \frac{4}{5} \\ 0 & 0 & 0 & 0 \\ -\frac{1}{10} & \frac{7}{10} & -\frac{1}{10} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0.06145 \\ 0.05370 \\ -0.4969 \\ 0 \\ -0.8640 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

A fin de facilitar los cálculos, multiplicamos miembro a miembro este sistema por *10*, para obtener el sistema equivalente:

$$\begin{pmatrix} -7 & -1 & -1 & 6 \\ -1 & -1 & 7 & 0 \\ 7 & 7 & 7 & 8 \\ 0 & 0 & 0 & 0 \\ -1 & 7 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0.6145 \\ 0.5370 \\ -4.969 \\ 0 \\ -8.640 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Para resolverlo, triangularemos la matriz ampliada del sistema:

$$\left(\begin{array}{cccc|c} -7 & -1 & -1 & 6 & 0.6145 \\ -1 & -1 & 7 & 0 & 0.5370 \\ 7 & 7 & 7 & 8 & -4.969 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 7 & -1 & 0 & -8.640 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Teniendo en cuenta que todas las operaciones se llevan a cabo en $\mathbb{R}$, utilizaremos el siguiente comando de Wolfram Mathematica *11.0* que triangula una matriz:

```
A = RowReduce[ { {-7,-1,-1,6,0.6145},{-1,-1,7,0,0.5370},{7,7,7,8,-4.969},{0,0,0,0,0},
{-1,7,-1,0,-8.640},{0,0,0,0,0},{0,0,0,0,0},{0,0,0,0,0} } ];
MatrixForm[A]
```

Al ejecutar el comando, obtenemos la siguiente matriz:

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0.286003 \\ 0 & 1 & 0 & 0 & -1.20115 \\ 0 & 0 & 1 & 0 & -0.0540203 \\ 0 & 0 & 0 & 1 & 0.226892 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vemos que $rango(A)=4$, ya que el número de filas no nulas de la matriz triangulada es *4*. Por lo tanto, el sistema tiene una única solución, que la llamaremos

$$(s_1,s_2,s_3,s_4)$$

Al resolver este sistema, obtenemos

$$(s_1,s_2,s_3,s_4)=(0.286003,-1.20115,-0.0540203,0.226892)$$

Como $s_1 \neq 0$, tomamos

$$(a,b,c,d)=\left(1,s_1^{-1}.\ s_3,s_1,s_2\right)=\left(1,\frac{-0.0540203}{0.286003},0.286003,-1.20115\right)=$$

$$=(1,-0.18888,0.286003,-1.20115)$$

Es decir

$$(a,b,c,d)=(1,-0.18888,0.286003,-1.20115)$$

<u>*Segundo Paso*</u>

Calculamos

$$k=(a.\ O_A+b)\ r_B\ (c.\ O_A+d)=(1.\ O_A-0.18888)\ r_B\ (0.286003\ O_A-1.20115)=$$
$$=(0.185007,-0.491784,0.0681793,0,-0.848078,0,0,0)$$

Por lo tanto,

$$k=(0.185007,-0.491784,0.0681793,0,-0.848078,0,0,0)$$

Ahora calculamos $[k.\ 256]$, que es un octonión que resulta de truncar la parte decimal de $k.\ 256$. Entonces

$$[k.\ 256]=[\ (0.185007,-0.491784,0.0681793,0,-0.848078,0,0,0).\ 256\ ]=$$
$$=[(256\times 0.185007,-256\times 0.491784,256\times 0.0681793,0,-256\times 0.848078,0,0,0)]=$$
$$=[(47.36,-125.89,17.453,0,-217.107,0,0,0)]=(47,-125,17,0,-217,0,0,0)$$

Luego, la clave K que comparten Alicia y Bernardo es

$$K = [k.\ 256] \pmod{256}$$

Es decir

$$K = (47,-125,17,0,-217,0,0,0) \equiv (47,131,17,0,39,0,0,0) \pmod{256}$$

Que expresado en forma de cuaternión es

$$K = (47,131,17,39) \pmod{256}$$

Como podemos comprobar en el Ejemplo *4.2*, es ésta la clave K que comparten Alicia y Bernardo.
Si bien en este Ejemplo hemos utilizado un comando prediseñado de Wolfram Mathematica para triangular una matriz, podemos diseñar un programa para tal fin. A continuación mostraremos cómo hacerlo.

El Método de Eliminación de Gauss en $\mathbb{R}$ aplicando Mathematica

El siguiente programa, diseñado mediante el software Wolfram Mathematica *11.0*, aplica el Método de Eliminación de Gauss a fin de triangular una matriz A de *8* filas y *5* columnas con coeficientes reales:

```
A = {{-7, -1, -1, 6, 0.6145}, {-1, -1, 7, 0, 0.5370}, {7, 7, 7, 8, -4.969},
   {0, 0, 0, 0, 0}, {-1, 7, -1, 0, -8.640}, {0, 0, 0, 0, 0}, {0, 0, 0, 0, 0},
   {0, 0, 0, 0, 0}};
For[i = 1, i ≤ 4, i++,
 If[A[[i, i]] == 0,
  (*Si A[[i,i]]=0, intercambio la k-ésima fila con la i-ésima*)
  Encontrado = 0;
  k = i + 1;
  While[Encontrado == 0 && k ≤ 8,
   If[A[[k, i]] ≠ 0,
    Encontrado = 1;
    Aux = A[[i]];
    A[[i]] = A[[k]];
    A[[k]] = Aux,
    k++;
   ]
  ]
 ];
 If[A[[i, i]] ≠ 0,
  (*Multiplicamos la i-ésima fila por el inverso de A[[i,i]] *)
```

```
  A[[i]] = 1/A[[i, i]] * A[[i]];
  For[j = i + 1, j ≤ 8, j++,
   A[[j]] = A[[j]] - A[[j, i]] * A[[i]]
  ];
 ]
]
Print["La matriz triangulada es:", MatrixForm[A]]
```

Conclusiones

"Los números son el principio de todas las cosas."

Pitágoras (569 a.C. – 475 a.C.)

A pesar de haber transcurrido más de dos mil años desde que Pitágoras pronunciara esta afirmación, su pensamiento adquiere cada día más vigencia.

Y es que la Matemática está presente en todas las ramas de la ciencia. Hasta los conceptos matemáticos más abstractos, encuentran una aplicación en situaciones de la vida real.

Tal es el caso de los cuaterniones y octoniones que, en virtud de la inspiración de Jorge Kamlofsky y Pedro Hecht, se utilizaron para generar algoritmos criptográficos, como el Protocolo HK17.

Gracias al aporte de estos autores, pudimos profundizar en el conocimiento y propiedades de estos números, que resultan ser una extensión de los números complejos. Si bien se descubrió un algoritmo de ataque que permite descifrar las claves generadas por el Protocolo HK17, su contribución sigue siendo muy valiosa.

Jorge Kamlofsky y Pedro Hecht nos muestran que la Matemática Pura y la Aplicada van de la mano, y que se necesitan mutuamente para el desarrollo tecnológico y científico de nuestros tiempos.

Finalmente, esperamos que los ejemplos propuestos en este trabajo ayuden a comprender los conceptos matemáticos abordados.

Referencias

[1] Diffie, W. & Hellman, M.E. "*New Directions in Cryptography*". IEE Transactions on Information Theory 22. Pp. *644-654*, *1976*.

[2] Hecht, P."*Un modelo compacto de Criptografía Asimétrica empleando Anillos no Conmutativos*". VII Congreso de Seguridad Informática CIBSI. Panamá, *2013*.

[3] Kamlofsky, J. & Hecht, J.P. "*A Diffie-Hellman Compact Model over Non-Commutative Rings using quaternions*". VIII Congreso de Seguridad Informática CIBSI. Quito (Ecuador), *2015*.

[4] Kamlofsky, J. & Hecht, J.P. "*Post-Quantum Cryptography: An Elementary and Compact Key Exchange Scheme Based on Octonions*". IX Congreso de Seguridad Informática CIBSI. Buenos Aires, *2017*.

[5] Haoyu, Lie, Renzhang, Liu, Qutaibah, Malluhi, Yanbin, Pan, Yongge, Wang & Tianyuan, Xie. "*Breaking HK17 in Practice*". Simposio Internacional IEEE sobre Teoría de la Información. Paris (Francia), *2019*.

[6] Prieto, Cecilia Andrea. "*Modelo compacto del algoritmo Diffie-Hellman utilizando cuaterniones".* Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, *2019*.

[7] López, María Fernanda. "*Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos".* Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, *2020*.

[8] Granado Peralta, S. "*Matemática Discreta*". Ed. CEIT. Buenos Aires, 2002.

[9] Armando O. Rojo. "*Álgebra* I". Ed. El Ateneo. Buenos Aires, 1975.