UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD IZTAPALAPA

División de Ciencias Básicas e Ingeniería

Maestría en Ciencias Matemáticas Aplicadas e Industriales

Cifrado de datos e intercambio de claves utilizando polinomios de Dickson

Por:

Leticia Peña Téllez

TESIS

Para la obtención del grado:

MAESTRIA EN CIENCIAS MATEMATICAS APLICADAS E INDUSTRIALES

Dirigida por:
Dr. José Noé Gutiérrez Herrera

México, Distrito Federal 19 de marzo de 2014.

UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD IZTAPALAPA

Casa abierta al tiempo

DIVISION DE CIENCIAS BASICAS E INGENIERIA

CIFRADO DE DATOS E INTERCAMBIO DE CLAVES UTILIZANDO POLINOMIOS DE DICKSON

Tesis que presenta
Leticia Peña Téllez
Para obtener el grado de
Maestría en Ciencias
(Matemáticas Aplicadas e Industriales)

Asesor: **Dr. José Noé Gutiérrez Herrera**

Jurado Calificador:

Presidente:	Dr. Horacio Tapia Recillas
Secretario:	Dr. Carlos Enrique Signoret Poillon
Vocal:	Dr. Rodolfo San Agustín Chi
Vocal:	Dr. José Noé Gutiérrez Herrera

México, Distrito Federal

19 de marzo de 2014.

AGRADECIMIENTOS

A mi familia por su gran apoyo, paciencia y cariño. En especial a mi esposo Honorio, padres Martin e Hilaria y hermanos Rogelio e Iveth.

Al Dr. José Noé Gutiérrez Herrera por su apoyo y paciencia en el desarrollo de este trabajo. Además de haber leído y corregido la versión inicial.

A los profesores de la UAM-Iztapalapa que contribuyeron en mi formación académica.

A los Doctores Horacio Tapia, Noé Gutiérrez, Carlos Signoret y Rodolfo San Agustín por haberse tomado el tiempo necesario para la revisión del trabajo.

A mis compañeros de la maestría, en especial a Mary y Raquel por su amistad.

Índice general

Resumen

La aparición de la informática y el uso masivo de las comunicaciones digitales han producido un número creciente de problemas de seguridad. El objetivo de la criptografía es el de proporcionar comunicaciones seguras (y secretas) sobre canales inseguros. Algunos de los problemas que la criptografía trata de resolver son el cifrado de datos y el intercambio de claves seguro a través de un medio inseguro.

En este trabajo se estudia un sistema de cifrado de datos basado en un tipo especial de polinomios, llamados polinomios de Dickson, con coeficientes en los enteros módulo n. Se analizan criterios para polinomios de permutación, con énfasis en las propiedades de los polinomios de Dickson. Se dan las condiciones necesarias para que se pueda transmitir información de manera segura usando este sistema de cifrado. Se incluye además un análisis detallado sobre la seguridad del mismo. También se describe un protocolo para el intercambio de claves basado en polinomios de Dickson, que permite acordar la clave a utilizar en cada comunicación. Se examina la seguridad del protocolo comparando con el protocolo más usado en la actualidad que es el de Diffie-Hellman, mismo que basa su seguridad en el problema del logaritmo discreto (análogamente se define el problema de Dickson discreto).

Introducción

Desde el comienzo de la humanidad ha sido necesario comunicar información de forma privada entre las personas interesadas. La criptografía se ocupa de este problema y otros relacionados. De particular importancia resultan hoy en día los problemas de intercambio de claves de forma segura en un canal inseguro, el cifrado de datos y la firma digital, entre otros. El sistema de cifrado conocido como RSA (cf. [23]), publicado en 1978 y actualmente de los más utilizados, permite resolver los últimos dos problemas mencionados.

Como parte de su tesis de doctorado en 1896, L. E. Dickson inició el estudio de una clase especial de polinomios, ahora conocidos como polinomios de Dickson, que son definidos de la siguiente manera: para $a \in A$, donde A es un anillo conmutativo con identidad, el polinomio de Dickson de primera clase y orden $k \in \mathbb{N}$ es el polinomio, con coeficientes enteros, donde $D_0(x, a) = 2$, y

$$D_k(x,a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}, \ k \geq 1$$

donde $\lfloor \frac{k}{2} \rfloor$ es el mayor entero menor o igual a $\frac{k}{2}$.

A partir de esta definición $D_k(x, 0) = x^k$ es el polinomio en el que está basado el sistema de cifrado RSA en los enteros modulares, por lo que este es un caso particular de los polinomios de Dickson.

En el presente trabajo se demuestra que para $n = \prod_{i=1}^{r} p_i^{e_i}$, con los p_i primos distintos, para $1 \leq i \leq r$ y $a \in \mathbb{Z}_n^*$, $D_k(x, a)$ es un polinomio de permutación de módulo n si y sólo si $\text{mcd}(k, \text{mcm}\left[p_1^{e_1-1}(p_1^2-1), \ldots, p^{e_r-1}(p_r^2-1)\right]) = 1$. Tal resultado demuestra la falsedad del teorema 2 que se presenta en [28], el cual afirma que $D_n(x, 1)$ es un polinomio de permutación módulo 2^m, $m \geq 2$ si y sólo si n es impar, como lo muestra el ejemplo 5. Además una consecuencia del teorema 2.12 es que el polinomio de Dickson $D_n(x, 1)$ es un polinomio de permutación módulo 2^m, $m \geq 2$ si y sólo si n es impar y no es múltiplo de 3, lo que caracteriza a los polinomios de Dickson que son de permutación módulo 2^m.

También en [28] se afirma que si $1 \leq n \in \mathbb{Z}$ y $D_n(x,1)$ es un polinomio de permutación módulo 2^m, entonces $D_{n+2}(x,1)$ es polinomio de permutación módulo 2^m. Por lo dicho en el párrafo anterior $D_7(x,1)$ es polinomio de permutación módulo 2^m pero $D_9(x,1)$ no lo es, por lo tanto el lema 3.3 del artículo [28] es falso. Se le añadieron algunas condiciones al enunciado de este resultado obteniendo el lema 2.6, que se expresa de la siguiente manera: sea k un entero positivo impar, si $D_k(x,1)$ es un polinomio de permutación módulo $n = 2^\omega$, con $\omega \geq 2$, $D_{k+1}(x,1) = \sum_{j=1}^{\lfloor \frac{k+1}{2} \rfloor} c_{2j} x^{2j}$ y $\sum_{j=1}^{\lfloor \frac{k+1}{2} \rfloor} c_{2j}$ es par, entonces $D_{k+2}(x,1)$ es también un polinomio de permutación módulo $n = 2^\omega$, con $\omega \geq 2$.

Se estudia un sistema de cifrado basado en polinomios de Dickson $D_n(x,1)$, mismo que fue presentado en 1981 por W.B. Muller y W. Nobauer (cf. [18]). Para elegir la llave de cifrado se hace de tal manera que el polinomio $D_n(x,1)$ sea polinomio de permutación módulo n; se muestra cómo cifrar el mensaje, la forma de elegir la llave de descifrado y cómo descifrar un mensaje utilizando este sistema de cifrado.

También se presentan algunos de los ataques más comunes al sistema de cifrado, y se dan las condiciones que debe cumplir n para que sea seguro ante tales ataques. Si n satisface las condiciones propuestas se tiene un sistema de cifrado al menos tan seguro como el RSA, por lo que es una opción para ser utilizada en su lugar, sólo que no es tan conocida a pesar de haber sido presentada tres años después que el RSA.

El intercambio de claves de forma segura en un canal inseguro es uno de los problemas importantes de la criptografía. En el presente escrito se estudia un protocolo similar al que se describe en [28] también basado en polinomios de Dickson. Se le hicieron las adecuaciones pertinentes a los resultados que se obtuvieron relacionados a polinomios de permutación de Dickson y a la función SHA-3, función hash estándar actualmente.

En el primer capítulo se define polinomio de permutación y se dan algunos criterios para decidir si un polinomio es de permutación primero en un campo finito $\mathbb{F}_q$, y posteriormente en el anillo $\mathbb{Z}_{2^\omega}$. Al revisar el lema 5 de [24] se encontraron contraejemplos (ver ejemplo 2), una versión modificada se presenta en el lema 1.13. En el segundo capítulo se muestra la fórmula de Waring a partir de la cual se definen los polinomios de Dickson, así como algunas de sus propiedades. El resultado más importante en este capítulo es el teorema 2.12, un resultado que nos permite obtener polinomios de permutación de Dickson, que son la base para un sistema de cifrado basado en ellos. En el tercer capítulo se estudian de manera especial los polinomios de permutación de Dickson que forman un grupo bajo la composición de polinomios. En el capítulo cuatro se presenta el sistema de cifrado basado en polinomios de Dickson, y algunos ataques a este sistema. En el quinto capítulo se revisa un protocolo de intercambio de claves basado en polinomios de Dickson, presentando un problema análogo al problema del logaritmo discreto, que

llamamos problema de Dickson discreto.

Capítulo 1

Polinomios de permutación

En este capítulo se define el concepto de polinomio de permutación y se dan algunos criterios para saber si un polinomios es de permutación (cf. [12]). Además se caracterizan los polinomios de permutación módulo 2^w (cf. [24], [27]).

1.1. Criterios para polinomios de permutación

En esta sección se da la definición de polinomio de permutación y se presentan algunos resultados importantes para determinar cuándo un polinomio es de permutación (cf. [12]), además de algunas de sus propiedades. Todos estos resultados serán de utilidad en el desarrollo posterior del presente trabajo.

Se considera al campo finito $\mathbb{F}_q$ con q elementos, donde $q = p^r$ para algún primo p y $r > 0$. En general estos campos se construyen considerando un polinomio irreducible $f(x)$ de grado r con coeficientes en $\mathbb{Z}_p$[1], y se define $\mathbb{F}_q = \mathbb{Z}_p[x]/ < f(x) >$, donde $\mathbb{Z}_p[x]$ denota el anillo de todos los polinomios con coeficientes en $\mathbb{Z}_p$, $< f(x) >$ denota el ideal generado por $f(x)$.

Definición 1. *Un polinomio $f \in \mathbb{F}_q[x]$ es llamado polinomio de permutación de $\mathbb{F}_q$ si la función polinomial asociada $c \longmapsto f(c)$ de $\mathbb{F}_q$ a $\mathbb{F}_q$ es una permutación de $\mathbb{F}_q$, es decir una función biyectiva de $\mathbb{F}_q$ en sí mismo.*

Obviamente, si f es un polinomio de permutación de $\mathbb{F}_q$, entonces la ecuación $f(x) = a$ tiene exactamente una solución en $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$. Por la finitud de $\mathbb{F}_q$, la definición de un polinomio de permutación puede ser expresado de varias formas.

Lema 1.1. *Sea $f \in \mathbb{F}_q[x]$ y considere $f : \mathbb{F}_q \to \mathbb{F}_q$. Entonces las siguientes condiciones son equivalentes:*

[1] $\mathbb{Z}_p$ es el anillo de enteros módulo p, al ser p primo se tiene que $\mathbb{Z}_p$ es campo.

i) $c \longmapsto f(c)$ *es una función inyectiva.*

ii) $c \longmapsto f(c)$ *es una función sobreyectiva.*

iii) $\forall a, a \in \mathbb{F}_q$, $f(x) = a$ *tiene una raíz en* $\mathbb{F}_q$.

iv) $\forall a, a \in \mathbb{F}_q$, $f(x) = a$ *tiene una única raíz en* $\mathbb{F}_q$.

Demostración. [iii) $\Leftrightarrow$ ii)] $\forall a, a \in \mathbb{F}_q$, existe $x \in \mathbb{F}_q$ tal que $f(x) = a$ si y sólo si f es sobreyectiva.

[iii) $\Leftrightarrow$ iv)] $\forall a, a \in \mathbb{F}_q$, si $f(x) = a$ tiene una raíz única en $\mathbb{F}_q$ para toda $a \in \mathbb{F}_q$, entonces $f(x) = a$ tiene una raíz en $\mathbb{F}_q$ para toda $a \in \mathbb{F}_q$.

Recíprocamente supongamos que $\forall a, a \in \mathbb{F}_q$, $f(x) = a$ tiene una raíz en $\mathbb{F}_q$, y que existe $b \in \mathbb{F}_q$ tal que $f(x) = b$ no tiene raíz única en $\mathbb{F}_q$. Sean $c_1, c_2 \in \mathbb{F}_q$ raíces distintas de $f(x) = b$, entonces $f(c) = b = f(d)$. Sin pérdida de generalidad, supongamos que existe $a \in \mathbb{F}_q$ tal que c es una raíz de $f(x) = a$, entonces $b = f(c) = a$, por lo tanto $a = b$. Así $\forall a \in \mathbb{F}_q$, $f(x) = a$ tiene una única raíz en $\mathbb{F}_q$.

[i) $\Leftrightarrow$ iv)] Supongamos que f es inyectiva y consideremos $a \in \mathbb{F}_q$ arbitrario tal que $f(x) = a$ no tiene raíz única, entonces existen $c_1, c_2 \in \mathbb{F}_q$ tales que $c_1 \neq c_2$ y $f(c_1) = f(c_2) = a$ lo que no puede ser pues f es inyectiva, por lo tanto f tiene raíz única.

Ahora supongamos que $\forall a, a \in \mathbb{F}_q$, $f(x) = a$ tiene una única raíz en $\mathbb{F}_q$ y que f no es inyectiva. Entonces pueden encontrarse $c_1, c_2 \in \mathbb{F}_q$ tales que $c_1 \neq c_2$ y $f(c_1) = f(c_2) = a_0$ lo que no puede ser pues $f(x) = a_0$ tiene solución única. Por lo tanto f es inyectiva. □

Del lema anterior puede deducirse una caracterización de los polinomios de permutación, como lo muestra el siguiente resultado.

Lema 1.2. *Un polinomio* $f \in \mathbb{F}_q$ *es un polinomio de permutación de* $\mathbb{F}_q$ *si y sólo si se cumple alguna de las siguientes condiciones:*

i) $c \longmapsto f(c)$ *es una función inyectiva.*

ii) $c \longmapsto f(c)$ *es una función sobreyectiva.*

iii) $\forall a \in \mathbb{F}_q$, $f(x) = a$ *tiene una raíz en* $\mathbb{F}_q$.

iv) $\forall a \in \mathbb{F}_q$, $f(x) = a$ *tiene una única raíz en* $\mathbb{F}_q$.

Demostración. Supongamos primero que f es un polinomio de permutación en $\mathbb{F}_q$, entonces $c \longmapsto f(c)$ es una permutación de $\mathbb{F}_q$, es decir $c \longmapsto f(c)$ es inyectiva y sobreyectiva, por lo que se cumplen i) y ii).

Por ser sobreyectiva $\forall a, a \in \mathbb{F}_q$, $f(x) = a$ tiene una raíz en $\mathbb{F}_q$, es decir se cumple iii).

Y iv) se cumple por la inyectividad de la función.

Ahora supongamos que se cumple alguna de las condiciones i) a iv). Por el lema 1.1 se tiene que las cuatro afirmaciones son equivalentes, es decir $c \longmapsto f(c)$ es biyectiva por lo que es una permutación en $\mathbb{F}_q$, y así f es un polinomio de permutación de $\mathbb{F}_q$. □

Si $\phi : \mathbb{F}_q \to \mathbb{F}_q$ es una función arbitraria de $\mathbb{F}_q$ sobre $\mathbb{F}_q$, entonces existe un único polinomio $g \in \mathbb{F}_q[x]$ con $gr(g) < q$ que representa a ϕ, en el sentido de que $\phi(c) = g(c)$ para todo $c \in \mathbb{F}_q$ (aquí $gr(g)$ representa el grado de g). El polinomio g puede encontrarse con ayuda del polinomio de interpolación de Lagrange para la función dada ϕ:

$$g(x) = \sum_{j=0}^{k} \phi(x_j)\ell_j(x),$$

donde $\ell_j(x) = \prod_{i=0, i\neq j}^{k} \frac{x-x_i}{x_j-x_i}$, o por

$$g(x) = \sum_{c\in\mathbb{F}_q} \phi(c)\left(1-(x-c)^{q-1}\right). \tag{1.1}$$

Nótese que:

$$1-(x-c)^{q-1} = \begin{cases} 1, & \text{si } x = c, \\ 0, & \text{si } x \neq c. \end{cases}$$

Por lo tanto $g(c) = \phi(c)$ para todo $c \in \mathbb{F}_q$.

Si ϕ está dada como una función polinomial, digamos $\phi : c \to f(c)$ con f en $\mathbb{F}_q[x]$, entonces g puede obtenerse de f al reducir módulo $x^q - x$ de acuerdo al siguiente resultado. De esta forma para analizar polinomios de permutación bastará con considerar únicamente aquellos de grado menor al orden del campo.

Lema 1.3. *Para $f, g \in \mathbb{F}_q[x]$ tenemos $f(c) = g(c)$ para toda $c \in \mathbb{F}_q$ si y sólo si*

$$f(x) \equiv g(x) \ (\textit{mód}\ x^q - x).$$

Demostración. Por el algoritmo de la división podemos escribir

$$f(x) - g(x) = h(x)(x^q - x) + r(x)$$

con $h, r \in \mathbb{F}_q[x]$ y $gr(r) < q$. Entonces $f(c) = g(c)$ si y sólo si

$$0 = h(c)(c^q - c) + r(c).$$

Como $c^q = c$, $\forall c, c \in \mathbb{F}_q$ (cf. [12]) esto sucede si y sólo si $r(c) = 0$. Así $r = 0$. Por lo que se cumple la conclusión deseada. □

Ahora vamos a establecer un criterio útil para polinomios de permutación. El siguiente lema será necesario para tal fin:

Lema 1.4. *Sean $a_0, a_1, \ldots, a_{q-1}$ elementos de $\mathbb{F}_q$. Entonces las siguientes dos condiciones son equivalentes:*

1. *$a_0, a_1, \ldots, a_{q-1}$ son distintos.*
2. $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{para } t = 0, 1, \ldots, q-2, \\ -1, & \text{para } t = q-1. \end{cases}$

Demostración. Considérese el polinomio

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j$$

para $1 \leq i \leq q-1$ y defina $g_0(x) = 1 - x^{q-1}$. Nótese que $g_0(0) = 1$ y $g_0(1) = 0$.

Ahora supóngase que $a_i \neq 0$, entonces $g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1} = 1 - q = 1$. Y si $b \neq a_i$ se cumple

$$g_i(b) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} b^j = 1 - \sum_{j=0}^{q-1} \left(a_i^{-1} b\right)^j = 1 - \frac{(a_i^{-1}b)^q - 1}{a_i^{-1}b - 1} = 1 - \frac{a_i^{-1}b - 1}{a_i^{-1}b - 1} = 0.$$

Por lo tanto se tiene la siguiente propiedad para el polinomio $g_i(x)$ con $0 \leq i \leq q-1$:

$$g_i(x) = \begin{cases} 1, & \text{si } x = a_i \\ 0, & \text{si } x \neq a_i. \end{cases} \tag{1.2}$$

esto es $g_i(x) = 1 - (x - a_i)^{q-1}$.

Se define el polinomio $g(x)$ como $g(x) = \sum_{j=0}^{q-1} g_j(x)$.

De la definición de $g_i(x)$ se siguen las siguientes igualdades:

$$g(x) = \sum_{i=0}^{q-1} \left(1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j\right) = q - \sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j} x^j\right) = -\sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j}\right) x^j.$$

Supóngase que $a_0, a_1, \ldots, a_{q-1}$ son distintos, entonces por (1.2)

$$g(a_i) = \sum_{j=0}^{q-1} g_j(a_i) = g_1(a_i) + \cdots + g_i(a_i) + \cdots + g_{q-1}(a_i) = g_i(a_i) = 1$$

para todo $0 \leq i \leq q-1$.

Ya que $gr(g) < q$, como consecuencia del lema 1.3 la imagen bajo g de cada elemento de $\mathbb{F}_q$ es 1 si y sólo si $g(x) = 1$ en $\mathbb{F}_q$.

Entonces

$$1 = g(x) = -\sum_{j=0}^{q-1}\left(\sum_{i=0}^{q-1} a_i^{q-1-j}\right)x^j = -\sum_{t=0}^{q-1}\left(\sum_{i=0}^{q-1} a_i^t\right)x^{q-1-t}$$

lo que es equivalente a que para $t = q-1$ se cumple $\sum_{i=0}^{q-1} a_i^t = -1$, y si $0 \leq t \leq q-2$ se tiene $\sum_{i=0}^{q-1} a_i^t = 0$ como se deseaba.

Recíprocamente si

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{para } t = 0, 1, \ldots, q-2, \\ -1, & \text{para } t = q-1, \end{cases}$$

se obtiene

$$g(x) = -\sum_{i=0}^{q-1} a_i^{q-1} - \sum_{j=1}^{q-1}\left(\sum_{i=0}^{q-1} a_i^{q-1-j}\right)x^j = -\sum_{i=0}^{q-1} a_i^{q-1} = 1.$$

Por tanto $g(a_i) = 1$ para todo $0 \leq i \leq q-1$, pero

$$g(a_i) = \sum_{j=0}^{q-1} g_j(a_i) = g_1(a_i) + \cdots + g_i(a_i) + \cdots + g_{q-1}(a_i) = 1.$$

Por (1.2) esto ocurre si para cada i exactamente uno de los sumandos $g_j(a_i)$, es igual a 1 y el resto son cero $0 \leq j \leq q-1$. Como para cada i, $0 \leq i \leq q-1$ se satisface $g_i(a_i) = 1$ no existe $j \neq i$ tal que $g_i(a_j) = g_i(a_i)$, de aquí $a_0, a_1, \ldots, a_{q-1}$ son distintos.

Con esto terminamos la demostración. □

El siguiente teorema enuncia uno de los resultados más útiles para determinar cuándo un polinomio representa una función biyectiva de un campo finito en sí mismo.

Teorema 1.5. *(**Criterio de Hermite** cf. [12]) Supóngase que $\mathbb{F}_q$ es de característica p. Entonces $f \in \mathbb{F}_q[x]$ es un polinomio de permutación de $\mathbb{F}_q$ si y sólo si se cumplen las siguientes condiciones:*

1. *f tiene exactamente una raíz en $\mathbb{F}_q$.*
2. *para cada entero t con $1 \leq t \leq q-2$ y $t \not\equiv 0$ (mód p), la reducción de $f(x)^t$ módulo $(x^q - x)$ tiene grado menor o igual a $q-2$.*

Demostración. Sea $f \in \mathbb{F}_q[x]$ un polinomio de permutación de $\mathbb{F}_q$, por el lema 1.2 se cumple que $f(x) = 0$ tiene exactamente una solución en $\mathbb{F}_q$, es decir (1.) se cumple.

Sea t un entero tal que $1 \leq t \leq q-2$ y $t \not\equiv 0$ (mód p). La reducción de $f(x)^t$ módulo $(x^q - x)$ es algún polinomio

$$g(x) = \sum_{j=0}^{q-1} {b_j}^t x^j$$

donde $b_{q-1}^t = -\sum_{c\in\mathbb{F}_q} f(c)^t$ por (1.1). De acuerdo al lema 1.4 se tiene que $b_{q-1}^t = 0$ para $t = 0, 1, \ldots, q-2$.

Por lo tanto $\sum_{j=0}^{q-1} b_j^t x^j = \sum_{j=0}^{q-2} b_j^t x^j + b_{q-1}^t x^{q-1}$. Así $g(x) = \sum_{j=0}^{q-2} b_j^t x^j$ tiene grado menor o igual a $q-2$.

Ahora supongamos que se cumplen (1.) y (2.). Entonces (1.) implica que $f(c) = 0$ para exactamente un $c \in \mathbb{F}_q$, y así

$$\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = 0 + 1 + 1 + \cdots + 1 = q - 1 = -1,$$

mientras (2.) implica $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ para $1 \le t \le q-2$ y $t \not\equiv 0 \pmod p$.

Y para $t = 0$, tenemos $\sum_{c\in\mathbb{F}_q} f(c)^0 = q = 0$.

Por lo tanto $\sum_{c\in\mathbb{F}_q} f(c)^t = \begin{cases} 0, & \text{si } 0 \le t \le q-2, \\ -1, & \text{si } t = q-1. \end{cases}$

Por el lema 1.4 $f(c_1), f(c_2), \ldots, f(c_{q-1})$ son todas distintas, lo que quiere decir que f es biyectiva y por lo tanto f es polinomio de permutación. □

Corolario 1.6. *Si $d > 1$ es un divisor de $q-1$, entonces no hay polinomios de permutación de $\mathbb{F}_q$ de grado d.*

Demostración. Supongamos que $f \in \mathbb{F}_q[x]$ es un polinomio de permutación con $gr(f) = d$, donde $gr(f)$ es el grado del polinomio $f(x)$. Entonces $1 \le \frac{q-1}{d} < q-1$, así $gr(f^{\frac{q-1}{d}}) = q-1$ lo que no puede ser porque la condición (2.) del teorema 1.5 no se satisface para $t = \frac{q-1}{d}$. Por lo tanto f no es polinomio de permutación. □

Se desprende de la demostración del teorema 1.5 que si $f \in \mathbb{F}_q[x]$ es un polinomio de permutación de $\mathbb{F}_q$, entonces la condición (2.) de dicho teorema se cumple también sin la restricción $t \not\equiv 0 \pmod p$. La condición (1.) puede sustituirse por otras condiciones, como por ejemplo la que se enuncia en el siguiente resultado:

Teorema 1.7. *Sea $\mathbb{F}_q$ un campo finito de característica p. Entonces $f \in \mathbb{F}_q[x]$ es un polinomio de permutación si y sólo si se cumplen las siguientes dos condiciones:*

1. *La reducción de $f(x)^{q-1}$ mód $(x^q - x)$ tiene grado $q-1$.*
2. *Para cada entero t con $1 \le t \le q-2$ y $t \not\equiv 0 \pmod p$, la reducción de $f(x)^t$ mód $(x^q - x)$ tiene grado menor o igual que $q-2$.*

Demostración. Supongamos primero que f es un polinomio de permutación, entonces (2.) se cumple por el Criterio de Hermite, en la notación de la demostración del mismo teorema tenemos

$$b_{q-1}^{q-1} = -\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = -(-1) = 1$$

y por lo tanto $\sum_{j=0}^{q-1} b_{q-1}^{q-1} x^j$ tiene grado $q-1$.

Ahora supongamos que se cumplen (1.) y (2.). Entonces como en la demostración del teorema 1.5 (2.) implica que $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ para $0 \leq t \leq q-2$, mientras (1.) implica que $\sum_{c\in\mathbb{F}_q} f(c)^{q-1}$ no es cero pues tiene grado $q-1$.

Por lo tanto el polinomio

$$g(x) = -\sum_{j=0}^{q-1} \left(\sum_{c\in\mathbb{F}_q} f(c)^{q-1-j} \right) x^j$$

no es cero. Si f no es polinomio de permutación, los valores $f(c), c \in \mathbb{F}_q$, no son todos distintos por lo que existe $b \neq f(c)$, $c \in \mathbb{F}_q$, tal que $g_i(b) = 0$ para todo i, y por lo tanto $g(b) = 0$ lo que contradice el hecho de que $g(x) \neq 0$.

Así f es polinomio de permutación. □

Del siguiente resultado pueden obtenerse algunos ejemplos de polinomios de permutación:

Teorema 1.8. *1. Cada polinomio lineal sobre $\mathbb{F}_q$ es un polinomio de permutación de $\mathbb{F}_q$.*

2. $f(x) = x^n$ es un polinomio de permutación de $\mathbb{F}_q$ si y sólo si $mcd(n, q-1) = 1$.

Demostración. **1.** Sea $f(x) = ax + b$ un polinomio lineal en $\mathbb{F}_q[x]$, con $a \neq 0$. Para c en $\mathbb{F}_q$ la ecuación $f(x) = c$ tiene solución única dada por $x = a^{-1}(c-b)$. Por el lema 1.2 f es un polinomio de permutación.

2. x^n es un polinomio de permutación si y sólo si la función $x \longmapsto x^n$ es inyectiva en $\mathbb{F}_q$, es decir $\left\{x^n : x \in \mathbb{F}_q^*\right\} = \mathbb{F}_q^{*2}$ lo que sucede si y sólo si $o(x^n) = q-1 = \frac{q-1}{mcd(n,q-1)}$, donde $o(x^n)$ es el orden de x^n en el grupo $\mathbb{F}_q^*$, pero esto es equivalente a decir que $mcd(n, q-1) = 1$. □

Ejemplo 1. Sea $q = 3^2$ y $q(x) = x^2 + 2x + 2$ un polinomio irreducible sobre $\mathbb{Z}_3$, así $\mathbb{F}_{3^2} = \mathbb{Z}[x]/\langle q(x)\rangle$. Sea α una raíz de $q(x)$ en $\mathbb{F}_{3^2}$, entonces los elementos de $\mathbb{F}_{3^2}$ son las potencias de α. Considérese $f(x) = 2x + 1$ y $g(x) = x^5$, de donde $(5, 3^2 - 1) = 1$. En la siguiente tabla se muestra la evaluación de $f(x)$ y $g(x)$ en $\mathbb{F}_{3^2}$.

[2] $\mathbb{F}_q^*$ denota el conjunto de elementos de $\mathbb{F}_q$ invertibles bajo el producto.

x	$f(x)$	$g(x)$
0	1	0
α	$2\alpha+1$	2α
$\alpha^2=\alpha+1$	2α	$\alpha+1$
$\alpha^3=2\alpha+1$	α	$\alpha+2$
$\alpha^4=2$	2	2
$\alpha^5=2\alpha$	$\alpha+1$	α
$\alpha^6=2\alpha+2$	$\alpha+2$	$2\alpha+2$
$\alpha^7=\alpha+2$	$2\alpha+2$	$2\alpha+1$
$\alpha^8=1$	0	1

De la tabla se puede observar que $f(x)$ y $g(x)$ son polinomios de permutación sobre $\mathbb{F}_q$, y además se cumple el teorema 1.8.

1.2. Polinomios de permutación módulo 2^ω

En está sección consideraremos polinomios de permutación sobre $\mathbb{Z}_n$, el anillo de los enteros módulo n, donde $n=2^\omega$, mismos que se consideran en [24] y [27]. El anillo $\mathbb{Z}_2$ es utilizado para la mayoría de las aplicaciones criptográficas de nuestro interés, pues las implementaciones se realizan eficientemente.

Comencemos con el caso $n=2$, es decir $\omega=1$.

Lema 1.9. *Un polinomio $f(x)=a_0+a_1x+\cdots+a_dx^d$ con coeficientes enteros es un polinomio de permutación módulo 2 si y sólo si $(a_1+a_2+\cdots+a_d)$ es impar.*

Demostración. Supongamos primero que f es polinomio de permutación módulo 2, entonces

$$\bar{f}(x)=\sum_{i=0}^{d}\bar{a}_ix^i\in\mathbb{Z}_2[x],$$

por lo que $\bar{a}_i=0$ ó 1, $0\leq i\leq d$.

Si $\bar{f}(\bar{0})=\bar{0}$, entonces $\bar{f}(\bar{1})=\bar{1}$. De la misma forma si $\bar{f}(\bar{0})=\bar{1}$, entonces $\bar{f}(\bar{1})=\bar{0}$. En cualquier caso $a_0+(a_0+a_1+a_2+\cdots+a_d)=\bar{1}$, lo que quiere decir que esta suma es impar.

Ahora supongamos que $(a_1+a_2+\cdots+a_d)=1$. De nuevo:

$$\bar{f}(x)=\sum_{i=0}^{d}\bar{a}_ix^i\in\mathbb{Z}_2[x]$$

de donde:

- si $\bar{f}(\bar{0})=\bar{0}$, entonces $\bar{f}(\bar{1})=\bar{0}+\bar{1}=\bar{1}$

- si $\bar{f}(\bar{0}) = \bar{1}$, entonces $\bar{f}(\bar{1}) = \bar{1} + \bar{1} = \bar{0}$

de aquí vemos que f es biyectiva, y por lo tanto f es un polinomio de permutación. □

Consideremos ahora el caso $n = 2^\omega$ con $\omega > 1$, para lo que se requiere una serie de resultados previos.

Lema 1.10. *Sea $f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbb{Z}_n[x]$ con $n = 2m$, donde m es un entero positivo par. Si f es un polinomio de permutación módulo n, entonces a_1 es impar.*

Demostración. Tenemos que $a_i 0^i \pmod{n} = 0$, para todo $i = 1, 2, \cdots, d$. Si a_1 fuera par, entonces $a_1 = 2s,\ s \in \mathbb{Z}$ y así $a_1 m^1 = 2sm \equiv 0 \pmod{2m}$ y como m es par entonces $m = 2t, t \in \mathbb{Z}$ de este modo para $i \geq 2$ se tiene que

$$a_i m^i = a_i (2t)^i = a_i 2^i t^i$$

y además $2m | a_i m^i$. Por lo tanto $a_i m^i \equiv 0 \pmod{n}$. Así $f(0) = a_0 = f(m)$ lo que no puede ser pues f es polinomio de permutación. Por lo tanto a_1 es impar. □

Lema 1.11. *Sea $f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbb{Z}_n[x]$ con $n = 2^\omega$, $\omega > 0$ y sea $m = 2^{\omega-1}$. Si f es un polinomio de permutación módulo n, entonces f es polinomio de permutación módulo m.*

Demostración. Supongamos que f no es polinomio de permutación módulo m, entonces existen $x, x' \in \mathbb{Z}_m$ tales que $x \neq x'$ y $f(x) = f(x') = y$ en $\mathbb{Z}_m$.

Nótese que $x,\ x',\ x + m,\ x' + m$ son valores diferentes en $\mathbb{Z}_n$.

Sea $Y = \{a \in \mathbb{Z}_n : a \equiv y \pmod{m}\} = \{y, y + m\}$, es decir Y lo podemos ver como $Y = \{f(x), f(x'), f(x + m), f(x' + m)\}$, y como $|Y| = 2$ se tiene: si $f(x) = f(x') = y$ en $\mathbb{Z}_n$ sería una contradicción pues f es polinomio de permutación en $\mathbb{Z}_n$. Luego $f(x) = f(x + m) = y$ en $\mathbb{Z}_n$, pero $x \neq x + m$ en $\mathbb{Z}_n$ lo que contradice que f es polinomio de permutación en $\mathbb{Z}_n$.

De la misma forma si $f(x') = f(x + m)$, entonces $f(x') = f(x' + m)$ o bien $f(x) = f(x' + m)$ en $\mathbb{Z}_n$.

Por lo tanto f es polinomio de permutación módulo m. □

Lema 1.12. *Sean $f(x) \in \mathbb{Z}[x]$ y $n = 2m$, tal que $f(x)$ no es constante y es un polinomio de permutación. Si f es un polinomio de permutación módulo n, entonces se cumple la congruencia polinomial $f(x + m) \equiv f(x) + m \pmod{n}$ para todo $x \in \mathbb{Z}_n$.*

Demostración. Para $x \in \mathbb{Z}_n$, se tiene la siguiente congruencia

$$f(x + m) \equiv f(x) \pmod{m}$$

entonces $f(x + m) - f(x) = mt, t \in \mathbb{Z}$. Si t es par, $f(x + m) - f(x) = 2ms$, es decir $f(x + m) \equiv f(x) \pmod{n}$ lo que contradice que f sea polinomio de permutación módulo n. Por lo tanto t es impar, digamos $t = 2s + 1, s \in \mathbb{Z}$, y así

$$f(x + m) - f(x) = 2ms + m = ns + m.$$

Luego $f(x+m) \equiv f(x) + m \pmod{n}$.

Por lo tanto $f(x+m) \equiv f(x) + m \pmod{n}$, para todo $x \in \mathbb{Z}_n$. □

En el artículo polinomios de permutación módulo 2^m (cf. [24]), se demuestra el lema 5 que afirma que el polinomio $f(x) = a_0 + a_1x + \cdots + a_dx^d$ con coeficientes enteros y $n = 2m$, donde m es par, si f es un polinomio de permutación módulo m entonces $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par si y sólo si f es polinomio de permutación módulo n, lo cual es falso como lo muestra el siguiente ejemplo:

Ejemplo 2. Sean $m = 2$ entonces $n = 2m = 4$. Considérese $f(x) = 3x^2 + 2x + 2$ donde $a_3 = 0$ por lo que es par.

Se tiene que en $\mathbb{Z}_2$: $f(0) = 0$ y $f(1) = 1$, con lo que f es polinomio de permutación módulo 2.

Pero en $\mathbb{Z}_4$ se tiene: $f(0) = f(2) = 2$ y $f(1) = f(3)$ por lo que $f(x)$ no es polinomio de permutación módulo 4.

Se añadió la condición a_1 impar al mencionado lema en [24], para corregir su falsedad, resultando el lema que se enuncia a continuación.

Lema 1.13. *Sean $f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbb{Z}[x]$ y $n = 2m$, donde m es par. Si f es un polinomio de permutación módulo m, entonces $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par y a_1 es impar si y sólo si f es polinomio de permutación módulo n.*

Demostración. Supongamos que f es polinomio de permutación módulo n, entonces por el lema 1.10 a_1 es impar, tenemos que $f(x+m) = \sum_{i=0}^{d} a_i(x+m)^i$, y por ser m par $m = 2s$, para un $s \in \mathbb{Z}$. Así para $i \geq 1$ y en $\mathbb{Z}_n$ se satisface

$$(x+m)^i = \sum_{k=0}^{i} \binom{i}{k} m^k x^{i-k} = x^i + imx^{i-1} + \sum_{k=2}^{i} \binom{i}{k} (4s)(2s)^{k-1} 2^{-1} x^{i-k} = x^i + imx^{i-1},$$

por lo que $a_i(x+m)^i \equiv a_ix^i + ia_imx^{i-1} \pmod{n}$ para $1 \leq i \leq d$.

Así que

$$f(x+m) \equiv f(x) + \sum_{i=1}^{d} ia_imx^{i-1} \pmod{n} \tag{1.3}$$

de donde, cuando x es par, se tiene

$$f(x+m) \equiv f(x) + a_1m \pmod{n} \tag{1.4}$$

como a_1 es impar, entonces $f(x+m) \equiv f(x) + m \pmod{n}$. Por otro lado si x es impar en $\mathbb{Z}_n$ se satisface:

$$f(x+m) = f(x) + a_1m + \sum_{i=2}^{d} ia_im = f(x) + a_1m + \sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}m. \tag{1.5}$$

Por el lema 1.12 se cumple que $f(x+m) \equiv f(x) + m \pmod{n}$ para todo $x \in \mathbb{Z}_n$. Cuando x es par se tiene la igualdad (1.4), y cuando x es impar se cumple que $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par.

Recíprocamente supongamos que a_1 es impar y la suma $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par. De (1.4) se tiene que para x par $f(x+m) \equiv f(x) + m \pmod{n}$ y de (1.5) cuando x es impar se satisface $f(x+m) \equiv f(x) + m \pmod{n}$.

Por lo tanto $f(x+m) \equiv f(x) + m \pmod{n}$ para todo $x \in \mathbb{Z}_n$.

Supongamos que existen $x, y \in \mathbb{Z}_n$ distintos tales que $f(x) \equiv f(y) \pmod{n}$, entonces $f(x) \equiv f(y) \pmod{m}$. Pero f es polinomio de permutación módulo m por lo que $x \equiv y \pmod{m}$ y se tienen los siguientes casos:

1. $y \equiv x \pmod{n}$
2. $y \equiv x + m \pmod{n}$

pero estamos suponiendo que $y \not\equiv x \pmod{n}$, por lo que $y \equiv x + m \pmod{n}$.

Entonces $f(y) \equiv f(x+m) \pmod{n} \equiv f(x) + m \pmod{n} \equiv f(y) + m \pmod{n}$, así que $m \equiv 0 \pmod{n}$, lo que no puede ser. Por lo tanto f es inyectiva sobre $\mathbb{Z}_n$. Por el lema 1.12, f es polinomio de permutación módulo n. □

Teorema 1.14. *Sea $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}[x]$. Entonces f es un polinomio de permutación módulo $n = 2^\omega, \omega \geq 2$, si y sólo si a_1 es impar, $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j}$ es par y $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par.*

Demostración. Supongamos que f es un polinomio de permutación módulo n, entonces por el lema 1.10, a_1 es impar. Además f es también un polinomio de permutación módulo $m = \frac{n}{2}$ por el lema 1.11, y $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par por el lema 1.13. Repetimos $\omega - 1$ veces el lema 1.11 hasta tener $m = 2$ y así f es un polinomio de permutación módulo 2, y por el lema 1.9 $\sum_{j=1}^{d} a_j$ es impar, pero a_1 es impar y $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par, entonces $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j}$ es par.

Ahora supóngase que a_1 es impar, $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par y $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j}$ es par.

Aplicaremos inducción sobre ω para demostrar que f es polinomio de permutación módulo $n = 2^\omega$.

Si $\omega = 2$, entonces $n = 4$ y $m = \frac{n}{2} = 2$, además se tiene que $\sum_{j=1}^{d} a_j$ es impar por lo que el lema 1.9 implica que f es polinomio de permutación módulo m.

Y como a_1 es impar, $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par se tiene por el lema 1.13 que f es un polinomio de permutación módulo $n = 2^\omega$.

Supóngase ahora que para $\omega \leq k$ se tiene que f es un polinomio de permutación módulo $n = 2^\omega$. Sea $\omega = k + 1$, por hipótesis de inducción f es polinomio de permutación módulo $m = 2^k$, a_1 es impar pero $\sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} a_{2j+1}$ es par se tiene del lema 1.13 que f es un polinomio de permutación módulo $n = 2^{k+1}$.

Por lo tanto f es polinomio de permutación módulo $n = 2^\omega$, como se deseaba. □

En seguida se dará una demostración alternativa al teorema 1.14, la cual se puede encontrar en [27], utilizando la derivada de polinomios. Antes de dar la demostración se prueban algunos resultados necesarios.

Consideramos las congruencias

$$f(x) \equiv 0 \pmod{p^a} \tag{1.6}$$

y

$$f(x) \equiv 0 \pmod{p^{a-1}} \tag{1.7}$$

donde $f(x) \in \mathbb{Z}[x]$, p es un número primo y $a > 1$.

Supongamos que x es una raíz de (1.6) con $0 \leq x < p^a$ Entonces x es de la forma $\varsigma + sp^{a-1}$ $(0 \leq s < p)$ donde ς es una raíz de (1.7) para la cual $0 \leq \varsigma < p^{a-1}$.

Por la fórmula de Taylor se tiene que

$$f(\varsigma + sp^{a-1}) = f(\varsigma) + sp^{a-1}f'(\varsigma) + \frac{1}{2}s^2p^{2a-2}f''(\varsigma) + \cdots \equiv f(\varsigma) + sp^{a-1}f'(\varsigma) \pmod{p^a}$$

ya que $ka - k \geq a$ para $k \geq 2$ y los coeficientes $\frac{f^{(k)}(\varsigma)}{k!}$ son enteros.

Ahora distinguimos 2 casos:

1. Supongamos que
$$f'(\varsigma) \not\equiv 0 \pmod{p} \tag{1.8}$$
entonces $\varsigma + sp^{a-1}$ es una raíz de (1.6) si y sólo si
$$f(\varsigma) + sp^{a-1}f'(\varsigma) \equiv 0 \pmod{p^a}.$$
Esta última igualdad es equivalente a $sf'(\varsigma) \equiv -\frac{f(\varsigma)}{p^{a-1}} \pmod{p}$ y existe una $s \in \mathbb{Z}_p$ que satisface esta condición.

2. Ahora si
$$f'(\varsigma) \equiv 0 \pmod{p} \tag{1.9}$$
se satisface $f(\varsigma + sp^{a-1}) \equiv f(\varsigma) \pmod{p^a}$. Si $f(\varsigma) \not\equiv 0 \pmod{p^a}$, entonces (1.6) no tiene solución. Y si $f(\varsigma) \equiv 0 \pmod{p^a}$, se cumple que $\varsigma + sp^{a-1}$ es una solución de (1.6) para cada s, y así hay p soluciones de (1.6) correspondientes a cada solución de (1.7).

De aquí se tiene el siguiente teorema.

Teorema 1.15. *El número de soluciones de (1.6) correspondientes a una solución ς de (1.7) es:*

(a) ninguna, si $f'(\varsigma) \equiv 0 \pmod{p}$ y ς no es una solución de (1.6).

(b) una, si $f'(\varsigma) \not\equiv 0 \pmod{p}$.

(c) p, si $f'(\varsigma) \equiv 0 \pmod{p}$ y ς es una solución de (1.6).

Demostración. Sea ς una solución de (1.7).

(a) Supóngase que $f'(\varsigma) \equiv 0 \pmod{p}$ y ς no es una solución de (1.6). Tenemos que $f(\varsigma + sp^{a-1}) \equiv f(\varsigma) + sp^{a-1}f'(\varsigma) \pmod{p^a}$, y como estamos suponiendo que $f'(\varsigma) \equiv 0 \pmod{p}$ se tiene $p^{a-1}f'(\varsigma) \equiv 0 \pmod{p^a}$. Además $p|f'(\varsigma)$ en consecuencia $p^a|p^{a-1}f'(\varsigma)$. Por lo tanto $f(\varsigma + sp^{a-1}) \equiv f(\varsigma) \pmod{p^a}$, y como ς no es solución de (1.6), entonces $f(\varsigma) \not\equiv 0 \pmod{p^a}$ y de esta manera se cumple $f(\varsigma + sp^{a-1}) \not\equiv 0 \pmod{p^a}$ para toda s tal que $0 \leq s < p$, por lo que (1.6) no tiene solución.

(b) Por otro lado si $f'(\varsigma) \not\equiv 0 \pmod{p}$ y $s,\ 0 \leq s < p$, es tal que el entero $\varsigma + sp^{a-1}$ es una raíz de (1.6), entonces $f(\varsigma) + sp^{a-1}f'(\varsigma) \equiv 0 \pmod{p^a}$. Supongamos que existe s' $(0 \leq s' < p)$ tal que $s \neq s'$ y $\varsigma + s'p^{a-1}$ es una raíz de (1.6), entonces $f(\varsigma) + sp^{a-1}f'(\varsigma) \equiv 0 \pmod{p^a}$ y se cumple sucesivamente que

$$\begin{aligned} f(\varsigma) + sp^{a-1}f'(\varsigma) &\equiv f(\varsigma) + s'p^{a-1}f'(\varsigma) \pmod{p^a} \\ sp^{a-1}f'(\varsigma) &\equiv s'p^{a-1}f'(\varsigma) \pmod{p^a} \\ sf'(\varsigma) &\equiv s'f'(\varsigma) \left(\text{mód } \frac{p^a}{(p^a, p^{a-1})}\right) \\ sf'(\varsigma) &\equiv s'f'(\varsigma) \pmod{p} \end{aligned}$$

como $f'(\varsigma) \neq 0 \pmod{p}$, entonces $s \equiv s' \pmod{p}$. Por lo tanto hay una solución única para (1.6).

(c) Por último supóngase que $f'(\varsigma) \equiv 0 \pmod{p}$ y ς es una solución de (1.6). Como se está suponiendo que $f'(\varsigma) \equiv 0 \pmod{p}$, entonces $p^{a-1}f'(\varsigma) \equiv 0 \pmod{p^a}$. Así $f(\varsigma + sp^{a-1}) \equiv f(\varsigma) \pmod{p^a}$. Por ser ς una solución de (1.6), entonces $f(\varsigma) \equiv 0 \pmod{p^a}$, así $f(\varsigma + sp^{a-1}) \equiv 0 \pmod{p^a}$ esto significa que $\varsigma + sp^{a-1}$ es una solución de (1.6) para cada valor de s y como $0 \leq s < p$, entonces hay p soluciones de (1.6). □

Como una consecuencia de este teorema obtenemos el siguiente resultado.

Corolario 1.16. *Sea p un primo. Entonces $f(x)$ permuta los elementos de $\mathbb{Z}_{p^n}, n > 1$ si y sólo si $f(x)$ permuta los elementos de $\mathbb{Z}_p$ y $f'(a) \not\equiv 0 \pmod{p}$ para toda $a \in \mathbb{Z}_p$.*

Demostración. Supongamos que f permuta los elementos de $\mathbb{Z}_{p^n}$ con $n > 1$, es decir, f es biyectiva en $\mathbb{Z}_{p^n}$. Entonces

$$f(x) \equiv 0 \pmod{p^n} \tag{1.10}$$

tiene exactamente una raíz, por (iv) del lema 1.2. Sea x tal raíz que además satisface

$$f(x) \equiv 0 \pmod{p}, \tag{1.11}$$

consideremos $x = \varsigma + sp,\ 0 \leq s < p^{n-1}$, donde ς es la raíz de (1.11) para la cual $0 \leq \varsigma < p$. Si hubiera otra solución ς' de (1.11) tal que se cumpliera la congruencia $f(\varsigma' + s'p) \equiv 0 \pmod{p^n}$, entonces $\varsigma' + s'p$ sería solución de (1.10) lo que no puede ser pues esta tiene solución única. Así ς es una raíz única de f en $\mathbb{Z}_p$ y por lo tanto f permuta a los elementos de $\mathbb{Z}_p$.

Por (b) del teorema 1.15 se tiene que $f'(\varsigma) \not\equiv 0 \pmod{p}$.

Ahora supóngase que ς es una raíz de (1.11) que satisface $0 \leq \varsigma < p$, además que $f'(\varsigma) \not\equiv 0 \pmod{p}$ y que $f(x)$ permuta a los elementos de $\mathbb{Z}_p$. Entonces por el teorema 1.15, $f(x) \equiv 0 \pmod{p^2}$ tiene exactamente una raíz correspondiente a la solución ς de (1.11). Repetimos esto hasta tener que $f(x) \equiv 0 \pmod{p^n}$ tiene exactamente una raíz correspondiente a la solución ς de (1.11) para cada $n > 1$, y de ahí se sigue que $f(x)$ permuta a los elementos de $\mathbb{Z}_{p^n}$. □

Ahora estamos en condiciones de dar la demostración alternativa al teorema 1.14.

Teorema 1.17. *Un polinomio $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ es un polinomio de permutación módulo 2^n, $n > 1$, si y sólo si a_1 es impar, $\sum_{i=1}^{\lfloor \frac{d}{2} \rfloor} a_{2i}$ es par y $\sum_{i=1}^{\lfloor \frac{d}{2} \rfloor} a_{2i+1}$ es par.*

Demostración. Por el corolario 1.16 $f(x)$ es un polinomio de permutación módulo 2^n si y sólo si $f(x)$ es un polinomio de permutación módulo 2 y $f'(x) \not\equiv 0 \pmod{2}$ para todo $x \in \mathbb{Z}_2$.

Además $f'(x) = \sum_{i=1}^{d} i a_i x^{i-1}$, como $0^i \equiv 0 \pmod{2}$ y $1^i \equiv 1 \pmod{2}$, entonces

$$f'(x) \equiv a_1 + \sum_{i=1}^{\lfloor \frac{d}{2} \rfloor} a_{2i+1} x \pmod{2}$$

Dado que se tiene $f'(x) \not\equiv 0 \pmod{2}$ para todo $x \in \mathbb{Z}_2$; en particular para $x = 0$ se satisface que a_1 es impar, y para $x = 1$ tenemos $a_1 + \sum_{i=1}^{\lfloor \frac{d}{2} \rfloor} a_{2i+1}$ es impar, pero a_1 es impar por lo que $\sum_{i=1}^{\lfloor \frac{d}{2} \rfloor} a_{2i+1}$ es par.

Por el lema 1.9 $f(x)$ es polinomio de permutación módulo 2 si y sólo si $\sum_{i=1}^{d} a_i$ es impar, por lo que $\sum_{i=1}^{\lfloor \frac{d}{2} \rfloor} a_{2i}$ es par. □

Capítulo 2

Polinomios de Dickson

En este capítulo se establecen algunos resultados que llevan a la fórmula de Waring (cf. [7]), a partir de la cual se definen los polinomios de Dickson.

Como parte de su tesis de doctorado en 1896, L. E. Dickson inició el estudio de una clase especial de polinomios, ahora conocidos como polinomios de Dickson (cf. [13]), algunas de sus propiedades que se demuestran en este capítulo nos permiten definir sistemas de cifrado de datos basados en ellos (cf. [19], [28]).

2.1. Funciones simétricas

En esta sección se definen las funciones simétricas y se muestran algunos ejemplos.

Sea $B[x_1, \ldots, x_n]$ el conjunto de polinomios en las indeterminadas $x_1, \ldots, x_n$, con coeficientes en un conjunto dado B. Definimos la acción de S_n, el grupo simétrico de n letras, en $B[x_1, \ldots, x_n]$ como

$$(\sigma, f) \longmapsto \sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Definición 2. *Se dice que f es simétrica si $\sigma \cdot f = f$ para todo $\sigma \in S_n$.*

Por ejemplo:

$$x_1^2 + x_2^2 + x_3^2 + 4x_1 + 4x_2 + 4x_3$$

es un polinomio simétrico en x_1, x_2, x_3. La suma de los primeros tres términos es denotado por $\sum x_i^2$ y la suma de los últimos tres términos por $4\sum x_i$.

En general, si t es una función racional en las indeterminadas $x_1, x_2, \ldots, x_n$, $\sum t$ denota la suma de t y de todas las funciones distintas obtenidas de t por permutaciones de las variables, tal que la función $\sum t$ es simétrica en $x_1, x_2, \ldots, x_n$.

Por ejemplo si existen 3 variables independientes α, β, γ

$$\sum \alpha\beta = \alpha\beta + \alpha\gamma + \beta\gamma$$

$$\sum \frac{1}{\alpha} = \frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma}$$

$$\sum \alpha^2\beta = \alpha^2\beta + \alpha^2\gamma + \beta^2\alpha + \beta^2\gamma + \gamma^2\alpha + \gamma^2\beta$$

En particular, $\sum \alpha = \alpha+\beta+\gamma$, $\sum \alpha\beta$, y $\alpha\beta\gamma$ son llamadas las tres funciones simétricas fundamentales en las indeterminadas α, β, γ.

En general

$$\sum \alpha_1, \sum \alpha_1\alpha_2, \sum \alpha_1\alpha_2\alpha_3, \ldots, \sum \alpha_1\alpha_2 \ldots \alpha_{n-1}, \alpha_1\alpha_2 \ldots \alpha_n$$

son las funciones simétricas fundamentales de $\alpha_1, \alpha_2, \ldots, \alpha_n$ y estas resultan ser (cf. [7]) respectivamente iguales a

$$-c_1, c_2, -c_3, \ldots, (-1)^n c_n$$

si $\alpha_1, \alpha_2, \ldots, \alpha_n$ son raíces de la ecuación

$$x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n = 0 \tag{2.1}$$

2.2. Suma de potencias de las raíces

La fórmula de Waring tiene que ver con la suma de potencias de raíces, en esta sección se analiza un polinomio de grado n y se calcula la suma de las k-ésimas potencias de las raíces del polinomio.

Consideremos el polinomio:

$$f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n \tag{2.2}$$

y sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(x)$.

Escribimos s_1 para $\sum \alpha_1$, s_2 para $\sum {\alpha_1}^2$ y en general

$$s_k = \sum \alpha_1^k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k$$

La forma factorizada de (2.2) es:

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) \tag{2.3}$$

calculamos la derivada y se obtiene

$$f'(x) = \sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \tag{2.4}$$

Si α es una raíz de $f(x)$ entonces, con $c_0 = 1$

$$\begin{aligned}
\frac{f(x)}{x-\alpha} &= \frac{f(x)-f(\alpha)}{x-\alpha} = \frac{x^n-\alpha^n}{x-\alpha} + c_1\frac{x^{n-1}-\alpha^{n-1}}{x-\alpha} + \cdots + c_{n-1}\frac{x-\alpha}{x-\alpha} \\
&= \sum_{i=0}^{n-1}\alpha^i x^{n-1-i} + c_1\sum_{i=0}^{n-2}\alpha^i x^{n-2-i} + \cdots + c_{n-1} \\
&= \sum_{i=0}^{n-1}\alpha^{n-1-i} x^i + c_1\sum_{i=0}^{n-2}\alpha^{n-2-i} x^i + \cdots + c_{n-1} \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1-i}\alpha^j c_{n-1-i-j}\right)x^i.
\end{aligned}$$

De esta manera

$$\frac{f(x)}{x-\alpha} = x^{n-1} + \sum_{k=1}^{n-1}\left(\alpha^k + c_1\alpha^{k-1} + \cdots + c_{k-1}\alpha + c_k\right)x^{n-k-1} \tag{2.5}$$

Tomando α sucesivamente como $\alpha_1, \alpha_2, \ldots, \alpha_n$, sumando los resultados y aplicando (2.4) obtenemos:

$$\begin{aligned}
f'(x) &= nx^n + (s_1 + nc_1)x^{n-2} + (s_2 + c_1s_1 + nc_2)x^{n-3} + \cdots \\
&+ (s_k + c_1s_{k-1} + c_2s_{k-2} + \cdots + c_{k-1}s_1 + nc_k)x^{n-k-1} + \cdots
\end{aligned}$$

Recuérdese que la derivada de (2.2) es

$$f'(x) = nx^{n-1} + (n-1)c_1x^{n-2} + (n-2)c_2x^{n-3} + \cdots + (n-k)c_kx^{n-k-1} + \cdots$$

Como esta expresión es idéntica a la anterior término por término, se tiene:

$$\begin{aligned}
&s_1 + c_1 = 0 \\
&s_2 + c_1s_1 + 2c_2 = 0 \\
&\vdots \\
&s_k + c_1s_{k-1} + c_2s_{k-2} + \cdots + c_{k-1}s_1 + kc_k = 0
\end{aligned} \tag{2.6}$$

Podemos encontrar a su vez $s_1, s_2, \ldots, s_{n-1}$ como:

$$\begin{aligned}
&s_1 = -c_1 \\
&s_2 = c_1^2 - 2c_2 \\
&s_3 = -c_1^3 + 3c_1c_2 - 3c_3 \\
&\vdots
\end{aligned} \tag{2.7}$$

Para encontrar s_n reemplazamos x en (2.2) por $\alpha_1, \alpha_2, \ldots, \alpha_n$ uno a la vez, sumamos las ecuaciones resultantes y obtenemos:

$$s_n + c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_{n-1} s_1 + n c_n = 0 \tag{2.8}$$

Al combinar (2.6) y (2.8) se obtiene

$$s_k + c_1 s_{k-1} + c_2 s_{k-2} + \cdots + c_{k-1} s_1 + k c_k = 0 \qquad 1 \leq k \leq n \tag{2.9}$$

El conjunto de fórmulas (2.7 - 2.9) es conocido como **Identidades de Newton**.

Para deducir una fórmula que nos permita calcular s_k para $k > n$, multiplicamos (2.2) por x^{k-n}, tomamos sucesivamente

$$x = \alpha_1, \ldots, x = \alpha_n$$

un valor a la vez, y sumamos las ecuaciones resultantes. De esta forma se obtiene la ecuación

$$s_k + c_1 s_{k-1} + c_2 s_{k-2} + \cdots + c_n s_{k-n} = 0 \qquad (k > n) \tag{2.10}$$

2.3. Fórmula de Waring

En la sección anterior se vio cómo encontrar $s_1, s_2, \ldots, s_k$, por las identidades de Newton. A veces es útil tener una expresión explícita para s_k, donde k tiene un valor arbitrario, la fórmula en cuestión se aplica habitualmente sólo a una ecuación cuadrática

$$x^2 + px + q = 0$$

En consecuencia vamos a tratar este caso con más detalle. Si sus raíces son α, β, entonces: $x^2 + px + q = (x - \alpha)(x - \beta)$.

Reemplazamos x por $\frac{1}{y}$ y multiplicamos por y^2, de donde se tiene :

$$1 + py + qy^2 = (1 - \alpha y)(1 - \beta y). \tag{2.11}$$

Calculando las derivadas respecto a y resulta

$$p + 2qy = -\alpha(1 - \beta y) - \beta(1 - \alpha y)$$

Combinando los signos y dividiendo por los miembros de (2.11) se deduce la siguiente ecuación

$$\frac{-p - 2qy}{1 + py + qy^2} = \frac{\alpha(1 - \beta y) + \beta(1 - \alpha y)}{(1 - \alpha y)(1 - \beta y)} = \frac{\alpha}{1 - \alpha y} + \frac{\beta}{1 - \beta y} \tag{2.12}$$

De $r^k - 1 = (r - 1)(r^{k-1} + r^{k-2} + \cdots + r + 1)$ se tiene la siguiente identidad:

$$\frac{1}{1 - r} = r^{k-1} + r^{k-2} + \cdots + r + 1 + \frac{r^k}{1 - r}. \tag{2.13}$$

Tomamos $r = \alpha y$ y multiplicando cada término del resultado por α, se tiene:

$$\frac{\alpha}{1-\alpha y} = \alpha + \alpha^2 y + \cdots + \alpha^k y^{k-1} + \frac{\alpha^{k+1} y^k}{1-\alpha y}.$$

De la misma forma si $r = \beta y$

$$\frac{\beta}{1-\beta y} = \beta + \beta^2 y + \cdots + \beta^k y^{k-1} + \frac{\beta^{k+1} y^k}{1-\beta y}.$$

Sea $\phi = \alpha^{k+1}(1-\beta y) + \beta^{k+1}(1-\alpha y)$, entonces:

$$\frac{\phi y^k}{(1-\alpha y)(1-\beta y)} = \frac{\alpha^{k+1} y^k}{1-\alpha y} + \frac{\beta^{k+1} y^k}{1-\beta y} = \frac{\phi y^k}{1+py+qy^2}.$$

Por lo tanto

$$\frac{\alpha}{1-\alpha y} + \frac{\beta}{1-\beta y} = s_1 + s_2 y + \cdots + s_k y^{k+1} + \frac{\phi y^k}{1+py+qy^2} \tag{2.14}$$

donde la expresión exacta para ϕ no es relevante.

A continuación se busca una expansión de la fracción en el miembro izquierdo de (2.12), su denominador será idéntico a la de (2.13), si hacemos $r = -py - qy^2$ en (2.13), entonces

$$\frac{1}{1+py+qy^2} = \frac{1}{1-(-py-qy^2)} = \sum_{t=0}^{k-1} (-1)^t (py+qy^2)^t + \frac{\psi y^k}{1+py+qy^2}$$

donde $\psi = (-p-qy^2)^k$, aunque no se va a hacer uso de la forma particular del polinomio ψ.

Por el Teorema del Binomio

$$(py+qy^2)^t = \sum \frac{(g+h)!}{g!h!} (py)^g (qy^2)^h$$

donde la suma se extiende sobre todo el conjunto de enteros no negativos g y h para los cuales $g+h=t$.

Por lo tanto

$$\frac{-p-2qy}{1+py+qy^2} = (p+2qy) \sum_{g+h \le k-1} (-1)^{g+h+1} \frac{(g+h)!}{g!h!} p^g q^h y^{g+2h} + E \tag{2.15}$$

donde $E = \frac{(-p-2qy)\psi y^k}{1+py+qy^2}$.

Como los miembros de (2.14) y (2.15) son idénticamente iguales por (2.12) sus lados derechos también lo son y los coeficientes de y^{k-1} son iguales.

Así el coeficiente s_k de y^{k-1} en (2.14) es igual al coeficiente de y^{k-1} en (2.15), por lo que se pueden separar en dos partes correspondientes a los términos del factor p y $2qy$.

Cuando se usa el término constante p, debemos emplear de (2.15) los términos en los cuales el exponente de y es $k-1$. Pero cuando se usa el término $2qy$, se requieren los términos donde el exponentes de y es $k-2$, para obtener y con exponente $k-1$, en ambos casos.

Por lo tanto s_k es igual a la suma de las siguientes dos partes:

$$p \sum_{g+2h=k-1} (-1)^{g+h+1} \frac{(g+h)!}{g!h!} p^g q^h$$

$$2q \sum_{g+2h=k-2} (-1)^{g+h+1} \frac{(g+h)!}{g!h!} p^g q^h$$

En la suma superior se consideran $i = g+1$ y $j = h$. En la suma inferior sea $i = g$, y $j = h+1$. Por lo tanto:

$$s_k = \sum_{i+2j=k} (-1)^{i+j} \frac{(i+j-1)!}{(i-1)!j!} p^i q^j + 2 \sum_{i+2j=k} (-1)^{i+j} \frac{(i+j-1)!}{i!(j-1)!} p^i q^j.$$

Finalmente podemos combinar nuestras dos sumas, multiplicamos el numerador y denominador de la primera fracción por i, y la segunda fracción por j. Así

$$s_k = k \sum_{i,j \geq 0, i+2j=k} (-1)^{i+j} \frac{(i+j-1)!}{i!j!} p^i q^j \tag{2.16}$$

Si reemplazamos i por su valor $k-2j$, y cambiamos el signo de p resulta que **la suma de las k-ésimas potencias de las raíces de** $x^2 - px + q = 0$ es igual a

$$\begin{aligned} s_k &= k \sum_{i,j \geq 0}^{\lfloor \frac{k}{2} \rfloor} (-1)^j \frac{(k-j-1)!}{(k-2j)!j!} p^{k-2j} q^j \qquad (2.17) \\ &= p^k - k p^{k-2} q + \frac{k(k-3)}{1 \cdot 2} p^{k-4} q^2 - \frac{k(k-4)(k-5)}{1 \cdot 2 \cdot 3} p^{k-6} q^3 + \cdots \end{aligned}$$

En esta ecuación cuadrática el producto de las raíces es igual a q. Por lo tanto si x denota una raíz, la segunda raíz es $\frac{q}{x}$. Esto es $s_k = x^k + \left(\frac{q}{x}\right)^k$.

La suma de las raíces es $x^k + \frac{q}{x} = p$, considerando que q es un valor dado y p es desconocido. De esta manera si c es una constante arbitraria, la ecuación

$$p^k - k p^{k-2} q + \frac{k(k-3)}{1 \cdot 2} p^{k-4} q^2 - \cdots = c \tag{2.18}$$

se transforma por la sustitución $p = x + \frac{q}{x}$ en $x^k + \left(\frac{q}{x}\right)^k = c$.

Se concluye que la ecuación (2.18) puede resolverse por radicales para p.

Para cualquier ecuación polinomial de la forma

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0$$

la fórmula para la suma de las k-ésimas potencias de sus raíces es:

$$s_k = k \sum (-1)^{r_1+r_2+\cdots+r_n} \frac{(r_1 + r_2 + \cdots + r_n - 1)!}{r_1! \cdots r_n!} c_1^{r_1} \cdots c_n^{r_n} \tag{2.19}$$

donde la suma se extiende sobre todo el conjunto de enteros $r_1, r_2, \cdots, r_n \geq 0$ y tal que $r_1 + 2r_2 + \cdots + nr_n = k$. Este resultado es conocido como la **fórmula de Waring** y fue publicado por él en 1762 (cf. [7]).

2.4. Definición de los polinomios de Dickson

En esta sección se definen los polinomios de Dickson, se muestra su relación con los polinomios de Chebyshev y se prueban algunas de sus propiedades. La exposición se hace siguiendo los resultados en [13] y [12].

Sean x_1, x_2 raíces de un polinomio de grado 2, entonces por la fórmula de Waring, podemos ver la suma de las k-ésimas potencias de estas raíces de la siguiente manera:

$$x_1^k + x_2^k = \sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \frac{k}{k-j} \binom{k-j}{j} (-x_1 x_2)^j (x_1 + x_2)^{k-2j}. \tag{2.20}$$

Esta igualdad se cumple para todo anillo conmutativo con identidad A, lo que justifica definir el **polinomio de Dickson** $D_k(x, a)$ sobre A con $a \in A$, como:

$$D_k(x, a) = \sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}.$$

Ejemplo 3. Sea $\mathbb{Z}_{15}$ el anillo de enteros módulo 15, a continuación se presentan los polinomios de Dickson de grado k, con $0 \leq k \leq 10$.

k	$D_k(x,a)$ mód 15
0	2
1	x
2	x^2+13
3	x^3+12x
4	x^4+11x^2+2
5	x^5+10x^3+5x
6	$x^6+9x^4+9x^2+13$
7	$x^7+8x^5+14x^3+8x$
8	$x^8+7x^6+5x^4+14x^2+2$
9	$x^9+6x^7+12x^5+9x$
10	$x^{10}+5x^6+5x^4+10x^2+13$

Ejemplo 4. Sea $\mathbb{Z}_7$ el anillo de enteros módulo 7, en la siguiente tabla se muestran los polinomios de Dickson de grado k, con $0 \leq k \leq 10$.

k	$D_k(x,a)$ mód 7
0	2
1	x
2	x^2+5
3	x^3+4x
4	x^4+3x^2+2
5	x^5+2x^3+5x
6	$x^6+x^4+2x^2+5$
7	x^7
8	$x^8+6x^6+6x^4+5x^2+2$
9	$x^9+5x^7+6x^5+5x^3+9$
10	$x^{10}+4x^8+6x^4+4x^2+5$

Cuando se trabaja sobre los números complejos los polinomios de Dickson están relacionados con los polinomios de Chebyshev de primer orden, los cuales se definen como: $T_k(x) = cos(k\ arccos\ x)$. Analicemos brevemente esta relación.

Si sustituimos $x_1 = e^{i\theta}$ y $x_2 = e^{-i\theta}$ en (2.20), se tiene

$$x_1^k + x_2^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-e^{i\theta}e^{-i\theta})^j (e^{i\theta} + e^{-i\theta})^{k-2j}$$

y así

$$x_1^k + x_2^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-1)^j (2\ cos\theta)^{k-2j} \tag{2.21}$$

Por otro lado

$$x_1^k + x_2^k = \left(e^{i\theta}\right)^k + \left(e^{-i\theta}\right)^k = 2\ cosk\theta \tag{2.22}$$

Haciendo $x = cos\theta$, de (2.21) y (2.22) se tiene la siguiente identidad

$$D_k(2x, 1) = 2\ T_k(x) \tag{2.23}$$

que es la conexión mencionada entre los polinomios de Dickson y los polinomios de Chebyshev. La identidad (2.23) puede utilizarse para definir los polinomios de Chebyshev de primer orden $T_k(x)$ sobre campos finitos de característica distinta de 2. Tales polinomios no son estudiados en el presente trabajo, pero en el último capítulo se les mencionará para hacer una comparación en la seguridad de un esquema de intercambio de claves.

Si consideramos un polinomio de Dickson $D_k(x, a)$ sobre un campo F, entonces en el campo de funciones racionales sobre F en la indeterminada y, sustituyendo $x_1 = y,\ x_2 = \frac{a}{y}$ en (2.20) tenemos:

$$\begin{aligned} y^k + \left(\frac{a}{y}\right)^k &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}\left(-y\left(\frac{a}{y}\right)\right)^j \left(y + \frac{a}{y}\right)^{k-2j} \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-a)^j \left(y + \frac{a}{y}\right)^{k-2j}. \end{aligned}$$

Por lo tanto

$$D_k\left(y + \frac{a}{y}, a\right) = y^k + \left(\frac{a}{y}\right)^k. \tag{2.24}$$

La definición de polinomios de Dickson nos lleva al siguiente resultado para $a, b \in F$ con $b \neq 0$:

$$D_k(x, ab^2) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-ab^2)^j x^{k-2j} = b^k \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-a)^j (b^{-1}x)^{k-2j}$$

De esta manera se obtiene la identidad:

$$D_k(x, ab^2) = b^k D_k(b^{-1}x, a) \tag{2.25}$$

Así que, si F es $\mathbb{F}_q$, el campo con q elementos, q par, entonces cada polinomio de Dickson $D_k(x, a),\ a \in \mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ puede ser expresado en términos de $D_k(x, 1)$, pues como la característica de $\mathbb{F}_q$ es 2, por el teorema 1.8 para toda $a \in \mathbb{F}_q^*$ existe $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, entonces por (2.25) se tiene que

$$D_k(x, a) = D_k(x, b^2) = b^k D_k(b^{-1}x, 1).$$

Si $F = \mathbb{F}_q$, q impar, entonces cada polinomio de Dickson $D_k(x, a),\ a \in \mathbb{F}_q^*$ puede ser expresado en términos de $D_k(x, 1)$ ó $D_k(x, c)$ donde c es fijo y no es un cuadrado en $\mathbb{F}_q$. Para que esto se cumpla tenemos 2 casos:

1. Si existe $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, entonces por (2.25) se tiene

$$D_k(x, a) = D_k(x, b^2) = b^k D_k(b^{-1}x, 1).$$

2. Cuando no existe $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, entonces existen $b, c \in \mathbb{F}_q^*$ tales que $a = b^2 c$, donde c no es un cuadrado en $\mathbb{F}_q$ [1]. Por lo tanto

$$D_k(x, a) = D_k(x, b^2 c) = b^k D_k(b^{-1}x, c).$$

Para q impar los polinomios de Dickson $D_k(x, a),\ a \in \mathbb{F}_q^*$ pueden ser expresados en términos de los polinomios de Chebyshev de primer orden $T_k(x)$ definidos por (2.23). Si $\beta \in \mathbb{F}_{q^2}$ es tal que $\beta^2 = a$, entonces (2.23) y (2.25) implican que

$$D_k(x, a) = \beta^k D_k(\beta^{-1}x, 1) = \beta^k \left(2T_k\left(\frac{\beta^{-1}x}{2}\right)\right) = 2\beta^k T_k\left((2\beta)^{-1}x\right)$$

Luego

$$\begin{aligned} D_k(x, a) &= \beta^k D_k(\beta^{-1}x, 1) \\ &= \beta^k \left(2T_k\left(\frac{\beta^{-1}x}{2}\right)\right) \\ &= 2\beta^k T_k\left((2\beta)^{-1}x\right) \end{aligned}$$

2.5. Propiedades de los polinomios de Dickson

Se muestran algunas propiedades de los polinomios de Dickson que se cumplen en cualquier anillo (cf. [13]), las cuales servirán de apoyo para la demostración de resultados que son de gran importancia para el desarrollo del presente trabajo.

Lema 2.1. *Sea $D_k(x, a)$ un polinomio de Dickson, entonces para $k \geq 2$ se satisface la siguiente relación de recurrencia:*

$$D_k(x, a) = xD_{k-1}(x, a) - aD_{k-2}(x, a) \tag{2.26}$$

con valores iniciales $D_0(x, a) = 2$ y $D_1(x, a) = x$.

[1] Notemos que si w es un generador de $\mathbb{F}_q^*$ y no existe $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, entonces $a = w^n$ con n impar. Es decir, $a = (w^t)^2 w$ donde $t \in \mathbb{N}$.

Demostración. Sea $x = u + \frac{a}{u}$, entonces por (2.24) se tiene

$$\begin{aligned} D_k(x,a) &= u^k + \left(\frac{a}{u}\right)^k \\ &= uu^{k-1} + \left(\frac{a}{u}\right)\left(\frac{a}{u}\right)^{k-1} + au^{k-2} - au^{k-2} + a\left(\frac{a}{u}\right)^{k-2} - a\left(\frac{a}{u}\right)^{k-2} \\ &= uu^{k-1} + \left(\frac{a}{u}\right)u^{k-1} + u\left(\frac{a}{u}\right)^{k-1} + \left(\frac{a}{u}\right)\left(\frac{a}{u}\right)^{k-1} - a\left[u^{k-2} + \left(\frac{a}{u}\right)^{k-2}\right] \\ &= \left(u + \frac{a}{u}\right)\left[u^{k-1} + \left(\frac{a}{u}\right)^{k-1}\right] - a\left[u^{k-2} + \left(\frac{a}{u}\right)^{k-2}\right] \\ &= xD_{k-1}(x,a) - aD_{k-2}(x,a). \end{aligned}$$

□

Lema 2.2. *Los polinomios de Dickson satisfacen las siguientes propiedades:*

1. $D_n(x,0) = x^n$.
2. $D_{mn}(x,a) = D_m\left(D_n(x,a), a^n\right)$.
3. *Si el anillo A tiene característica p, con p primo, se cumple la igualdad $D_{np}(x,a) = (D_n(x,a))^p$.*

Demostración. 1. De la definición de polinomio de Dickson se sigue que

$$D_n(x,0) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j}\binom{n-j}{j}(0)^j x^{n-2j} = x^n.$$

2. Sea $x = u + \frac{a}{u}$, entonces se tiene

$$\begin{aligned} D_{mn}(x,a) &= D_{mn}(u + \frac{a}{u}, a) = u^{mn} + \left(\frac{a}{u}\right)^{mn} = (u^n)^m + \left(\frac{a^n}{u^n}\right)^m \\ &= D_m\left(u^n + \left(\frac{a}{u}\right)^n, a^n\right) = D_m\left(D_n(x,a), a^n\right). \end{aligned}$$

3. Como en el inciso anterior se considera $x = u + \frac{a}{u}$, así que

$$D_{np}(x,a) = D_{np}(u + \frac{a}{u}, a) = u^{np} + \left(\frac{a}{u}\right)^{np} = \left[u^n + \left(\frac{a}{u}\right)^n\right]^p = \left(D_n(x,a)\right)^p.$$

□

2.6. Polinomios de permutación en un campo finito

En esta sección se demuestra un resultado que nos dice cuándo los polinomios de Dickson son de permutación, mismo que se usa posteriormente para poder decidir si un polinomio es de permutación en un anillo (cf. [12]).

Teorema 2.3. *El polinomio de Dickson $D_k(x,a),\ a \in \mathbb{F}_q^*$ es un polinomio de permutación de $\mathbb{F}_q$ si y sólo si mcd $(k, q^2-1) = 1$.*

Demostración. Supongamos primero que $mcd(k, q^2-1) = 1$. Sean $b, c \in \mathbb{F}_q$ tales que $D_k(b,a) = D_k(c,a)$. Podemos encontrar $\beta, \gamma \in \mathbb{F}_{q^2}$ soluciones de $x + ax^{-1} = b$ y $x + ax^{-1} = c$, respectivamente.

Entonces por (2.24) se cumple la igualdad $\beta^k + a^k\beta^{-k} = \gamma^k + a^k\gamma^{-k}$, que puede reescribirse como

$$\left(\beta^k - \gamma^k\right)\left(\beta^k\gamma^k - a^k\right) = 0.$$

Así $\beta^k - \gamma^k = 0$ ó $\beta^k\gamma^k - a^k = 0$, es decir $\beta^k = \gamma^k$ ó $\beta^k = \frac{a^k}{\gamma^k} = \left(a\gamma^{-1}\right)^k$. Como $mcd(k, q^2-1) = 1$, el teorema 1.8 implica que x^k es un polinomio de permutación en $\mathbb{F}_{q^2}$ de donde $\beta = \gamma$ ó $\beta = a\gamma^{-1}$, por lo que

1. si $\beta = \gamma$, entonces $b = c$.

2. si $\beta = a\gamma^{-1}$, entonces $\gamma = a\beta^{-1}$ y así $b = c$.

Por lo tanto $D_k(x,a)$ es un polinomio de permutación de $\mathbb{F}_q$.

Ahora supóngase que $D_k(x,a)$ es un polinomio de permutación de $\mathbb{F}_q$ y que $mcd(k, q^2-1) = d > 1$.

Si d es par, entonces q es impar y k es par. La ecuación de la definición de polinomios de Dickson muestra que $D_k(x,a)$ contiene sólo potencias pares de x, y así tenemos $D_k(c,a) = D_k(-c,a)$ para $c \in \mathbb{F}_q^*$, pero $c \neq -c$ lo que no puede ser pues $D_k(x,a)$ es polinomio de permutación de $\mathbb{F}_q$. Así que d es impar.

Como d es impar y existe un primo impar r tal que $r|d$, entonces $r|k$ y $r|(q^2-1)$. Como $r|(q^2-1)$, entonces $r|(q+1)$ ó $r|(q-1)$.

Ahora si $r|(q-1)$, entonces la ecuación $x^r = 1$ tiene r soluciones en $\mathbb{F}_q$, por lo que existe $b \in \mathbb{F}_q,\ b \neq 1$ y $b \neq a$, tal que $b^r = 1$ y así también $b^k = 1$ además por (2.24)

$$D_k(b + ab^{-1}, a) = b^k + \frac{a^k}{b^k} = 1^k + \frac{a^k}{1^k} = D_k(1+a, a).$$

Si se tiene $b + ab^{-1} = 1 + a$, al multiplicar por b ambos lados de la igualdad se obtiene $b^2 + a - b - ab = 0$, factorizando resulta $(b-1)(b-a) = 0$. Por lo tanto $b = 1$ ó $b = a$ lo que no puede ser, así que $b + ab^{-1} \neq 1 + a$, es decir $D_k(x,a)$ no es polinomio de permutación de $\mathbb{F}_q$ lo que también es una contradicción. Así que $r|(q+1)$. Sea $\gamma \in \mathbb{F}_{q^2}$ una solución

de $x^{q+1} = a$. Como $x^r = 1$ tiene r soluciones en $\mathbb{F}_{q^2}$, existe $\beta \in \mathbb{F}_{q^2},\ \beta \neq 1$ y $\beta \neq a\gamma^2$ con $\beta^r = 1$. Y además $\beta^{q+1} = 1$ y $\beta^k = 1$, y se tiene

$$D_k(\gamma + a\gamma^{-1}) = \gamma^k + \frac{a^k}{\gamma^k} = (\beta\gamma)^k + \frac{a^k}{(\beta\gamma)^k} = D_k(\beta\gamma + a\,(\beta\gamma)^{-1}, a).$$

Sin embargo en $\mathbb{F}_{q^2}$ se cumple $\gamma + a\gamma^{-1} = \gamma + (\gamma^{q+1})\,\gamma^{-1} = \gamma + \gamma^q$ y además $\beta\gamma + a\,(\beta\gamma)^{-1} = \beta\gamma + \gamma^{q+1}\,(\beta\gamma)^{-1} = \beta\gamma + (\beta\gamma)^{q+1}\,(\beta\gamma)^{-1} = \beta\gamma + (\beta\gamma)^q$.

Si $\beta\gamma + a\,(\beta\gamma)^{-1} = \gamma + a\gamma^{-1}$ se multiplica ambos lados por $\beta\gamma$ y se obtiene $(\beta\gamma)^2 - (\beta\gamma)\gamma + a - a\beta = 0$, factorizando resulta

$$\beta\gamma^2(\beta - 1) - a(\beta - 1) = (\beta - 1)(\beta\gamma^2 - a) = 0.$$

Entonces $\beta = 1$ ó $\beta = a\gamma^{-2}$ lo cual no puede ser, de ahí que $D_k(x, a)$ no es un polinomio de permutación de $\mathbb{F}_q$, lo que tampoco es posible. Por lo tanto $mcd(k, q^2 - 1) = d = 1$. □

Teorema 2.4. *Sea el polinomio de Dickson $D_n(x, a)$ con $a \neq 0$ un polinomio de permutación de $\mathbb{F}_q$. Entonces la derivada $D'_n(x, a) \neq 0$ en $\mathbb{F}_q$ si y sólo si $(n, q) = 1$.*

Demostración. Si $n = 1$, se tiene que $D_1(x, a) = x$ y $D'_1(x, a) = 1$, es decir se cumple el teorema. Así que supóngase $(n, q) = 1$ y $n > 1$, considere $x = y + \frac{a}{y}$ con $y \in \mathbb{F}^*_{q^2}$, entonces

$$D_n(x, a) = D_n\left(y + \frac{a}{y}, a\right) = y^n + \left(\frac{a}{y}\right)^n.$$

Aplicando la regla de la cadena para calcular la derivada de $D_n\left(y + \frac{a}{y}, a\right)$ y considerando que $\frac{\mathrm{d}x}{\mathrm{d}y} = 1 - \frac{a}{y^2}$, se tiene

$$\begin{aligned} D'_n\left(y + \frac{a}{y}, a\right) &= \frac{\mathrm{d}D_n}{\mathrm{d}y}\frac{\mathrm{d}y}{\mathrm{d}x} = \left[ny^{n-1} - n\left(\frac{a}{y}^{n-1} ay^{-2}\right)\right]\frac{1}{\frac{\mathrm{d}x}{\mathrm{d}y}} \\ &= \left[ny^{n-1} - n\left(\frac{a}{y}^{n-1} ay^{-2}\right)\right]\frac{1}{1 - \frac{a}{y^2}} \\ &= n\left[\frac{y^{2n} - a^{n-1}a}{y^{n+1}}\right]\frac{y^2}{y^2 - a} \\ &= \frac{ny^2(y^{2n} - a^n)}{y^{n-1}y^2(y^2 - a)} = \frac{n(y^{2n} - a^n)}{y^{n-1}(y^2 - a)}. \end{aligned}$$

Por lo tanto

$$D'_n\left(y + \frac{a}{y}, a\right) = \frac{n(y^{2n} - a^n)}{y^{n-1}(y^2 - a)}. \tag{2.27}$$

Esto es suficiente para mostrar que $D'_n(y + \frac{a}{y}, a) = 0$ no tiene solución en $\mathbb{F}_{q^2}$ o equivalentemente que el polinomio

$$\frac{n(y^{2n} - a^n)}{y^{n-1}(y^2 - a)} = 0 \tag{2.28}$$

no tiene raíces en $\mathbb{F}_{q^2}$.

Si $h(y) = y^{2n} - a^n$ y β es una raíz de $h(y)$, se mostrará que β es una raíz simple la cual satisface $y^2 - a = 0$.

La derivada de $h(y)$ es $h'(y) = 2ny^{2n-1}$, y se tienen 2 casos:

- Si q es impar, entonces $(h'(y), h(y)) = 1$ y por lo tanto $h(y)$ tiene únicamente raíces simples (cf. [12]). De forma similar $y^2 - a$ tiene sólo raíces simples pues $(y^2 - a, 2y) = 1$. Como $D_n(x, a)$ es un polinomio de permutación de $\mathbb{F}_q$ el teorema 1.8 implica que $(n, q^2 - 1) = 1$ para que y^n sea de polinomio de permutación en $\mathbb{F}_{q^2}$. Entonces si $\beta^{2n} = a^n$ se tiene que $\beta^2 = a$, es decir β es una raíz simple del numerador y denominador de (2.28).

- Para q par

  $$\frac{y^{2n} - a^n}{y^2 - a} = \left[\frac{y^n - \beta^n}{y - \beta}\right]^2$$

  donde $\beta^2 = a$. Como $(n, q^2 - 1) = 1$, entonces y^n es polinomio de permutación de $\mathbb{F}_{q^2}$ por lo que $y^n - \beta^n = 0$ tiene solución única y es $y = \beta$. Además la derivada de $y^n - \beta^n$ es ny^{n-1}, se ve que $y = \beta \neq 0$ es una raíz simple.

Por lo que (2.27) no tiene raíces en $\mathbb{F}_{q^2}$. □

2.7. Polinomios de Dickson mód 2^ω

Notemos que el polinomio de Dickson de primer orden $D_1(x, 1) = x$ es un polinomio de permutación mód $n = 2^\omega$, con $\omega \geq 1$, pues es la función identidad que es biyectiva. En esta sección se estudian condiciones bajo las que otros polinomios $D_k(x, 1)$ son de permutación módulo una potencia de dos.

Comenzamos con un lema que nos permite descartar muchos de los polinomios de Dickson (cf. [28]).

Lema 2.5. *El polinomio de Dickson $D_k(x, 1)$ de grado par no es un polinomio de permutación módulo $n = 2^\omega$, con $\omega \geq 2$.*

Demostración. Sea $k \geq 0$ un entero par, y el polinomio de Dickson de grado k como en la definición:

$$D_k(x, 1) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k - j} \binom{k - j}{j} (-1)^j x^{k-2j} \tag{2.29}$$

suponga que $D_k(x,1)$ es polinomio de permutación módulo $n=2^\omega$ con $\omega \geq 2$. Como k es par entonces $k-2j$ es par para todo j, por lo tanto x^{k-2j} es de grado par y así $D_k(x,1)$ sólo tiene términos de grado par, lo que contradice el teorema 1.17. Por lo tanto $D_k(x,1)$ con k par no es polinomio de permutación módulo $n=2^\omega$, con $\omega \geq 2$. □

Al desarrollar el lado derecho del polinomio de Dickson en (2.29) se obtiene una expresión de la siguiente forma

$$D_k(x,1) = \sum_{j=0}^{k} a_j x^j,$$

y por el lema anterior si k es par, entonces

$$D_k(x,1) = \sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor} a_{2j} x^{2j}.$$

El siguiente resultado se obtuvo de observar la listas de polinomios de Dickson, y tratar de caracterizarlos.

Lema 2.6. *Para $k \geq 1$, se cumple $D_{2k}(x,1) = \sum_{j=1}^{k} a_{2j} x^{2j} + a_0$, donde*

$$a_0 = (-1)^k 2$$

Demostración. La prueba se hace por inducción sobre k.

Si $k=1$ se tiene, por (2.26), que $D_2(x,1) = x^2 - 2$ de donde $a_0 = -2 = (-1)2$. Supongamos que para $k \leq t$ se cumple que

$$a_0 = (-1)^t 2.$$

Sea $k = t+1$, utilizando (2.26) se tiene que

$$D_{2(t+1)}(x,1) = D_{2t+2}(x,1) = xD_{2t+1}(x,1) - D_{2t}(x,1) = xD_{2t+1}(x,1) - \left(\sum_{j=1}^{2t} a_j x^j \right) - a_0$$

por lo que $D_{2(t+1)}(x,1) = \sum_{j=1}^{2(t+1)} b_j x^j$, donde $b_0 = -a_0 = -(-1)^t 2 = (-1)^{t+1} 2$. □

Como consecuencia de este lema se tiene que si $D_k(x,1) = \sum_{j=0}^{k} a_j x^j$, con k par, entonces a_0 es par.

Los polinomios de Dickson con grados $0 \leq k \leq 10$ y $a=1$ son:

k	$D_k(x,1)$
0	2
1	x
2	x^2-2
3	x^3-3x
4	x^4-4x^2+2
5	x^5-5x^3+5x
6	$x^6-6x^4+9x^2-2$
7	$x^7-7x^5+14x^3-7x$
8	$x^8-8x^6+20x^4-16x^2+2$
9	$x^9-9x^7+27x^5-30x^3+9x$
10	$x^{10}-10x^8+35x^6-50x^4+25x^2-2$

Ejemplo 5. De la tabla anterior los polinomios de Dickson módulo 2^2 son:

k	$D_k(x,1)$ mód 2^2
0	2
1	x
2	x^2+2
3	x^3+x
4	x^4+2
5	x^5+3x^3+x
6	$x^6+2x^4+x^2+2$
7	$x^7+x^5+2x^3+x$
8	x^8+2
9	$x^9+3x^7+3x^5+2x^3+x$
10	$x^{10}+2x^8+3x^6+2x^4+x^2+2$

Utilizando el teorema 1.17 $D_5(x,1)$ y $D_7(x,1)$ mód 2^2 son polinomios de permutación módulo 2^2, por otro lado $D_8(x,1)$ y $D_9(x,1)$ no son polinomios de permutación mód 2^2, pues en $D_8(x,1)$ mód 2^2 el valor de a_1 es 0 y en $D_9(x,1)$ mód 2^2 la suma $1+3+3+2$ es impar.

El siguiente resultado permite encontrar polinomios de permutación de Dickson si ya se conoce alguno, y en relación al resultado original que se da en [28], a este se le añadió la siguiente condición: $D_{k+1}(x,1)=\sum_{j=1}^{\lfloor\frac{k+1}{2}\rfloor}c_{2j}x^{2j}$ y $\sum_{j=1}^{\lfloor\frac{k+1}{2}\rfloor}c_{2j}$ es par, pues del ejemplo 5 $D_8(x,1)$ no satisface que $\sum_{j=1}^{\lfloor\frac{k+1}{2}\rfloor}c_{2j}$ es par y aunque $D_7(x,1)$ es polinomio de permutación mód 2^2 se puede verificar fácilmente que $D_9(x,1)$ no es polinomio de permutación mód 2^2. Es decir el resultado que aparece en [28] es falso.

Lema 2.7. *Sea k un entero positivo impar. Si $D_k(x,1)$ es un polinomio de permutación módulo $n=2^\omega$, con $\omega\geq 2$, $D_{k+1}(x,1)=\sum_{j=1}^{\lfloor\frac{k+1}{2}\rfloor}c_{2j}x^{2j}$ y $\sum_{j=1}^{\lfloor\frac{k+1}{2}\rfloor}c_{2j}$ es par, entonces $D_{k+2}(x,1)$ es también un polinomio de permutación módulo $n=2^\omega$, con $\omega\geq 2$.*

Demostración. Sea $D_k(x,1) = \sum_{j=0}^{k} a_j x^j$ y $D_{k+2} = \sum_{j=0}^{k+2} b_j x^j$. Como $D_k(x,1)$ es un polinomio de permutación módulo $n = 2^\omega$ con $\omega \geq 2$, por el teorema 1.17, a_1 es impar, $\sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} a_{2j}$ es par y $\sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} a_{2j+1}$ es par.

Por (2.26) $D_{k+2}(x,1) = xD_{k+1}(x,1) - D_k(x,1)$, es decir

$$\begin{aligned}\sum_{j=0}^{k+2} b_j x^j &= x \sum_{j=1}^{\lfloor \frac{k+1}{2} \rfloor} c_{2j} x^{2j} - \sum_{j=0}^{k} a_j x^j = \sum_{j=1}^{\lfloor \frac{k+1}{2} \rfloor} c_{2j} x^{2j+1} - \sum_{j=0}^{k} a_j x^j \\ &= c_{k+1} x^{k+1} + \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (c_{2j} - a_{2j+1}) x^{2j+1} + \sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} a_{2j} x^{2j}.\end{aligned}$$

Así

1. $b_1 = c_0 - a_1$, por el lema 2.6 c_0 es par y por hipótesis a_1 es impar, de ahí que b_1 sea impar.
2. $\sum_{j=1}^{\lfloor \frac{k+2}{2} \rfloor} b_{2j} = \sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} a_{2j}$ es par por hipótesis.
3. $\sum_{j=1}^{\lfloor \frac{k+2}{2} \rfloor} b_{2j+1} = \sum_{j=1}^{\lfloor \frac{k+1}{2} \rfloor} c_{2j} - \sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} a_{2j+1}$, donde por hipótesis el primero y segundo sumando son pares, entonces $\sum_{j=1}^{\lfloor \frac{k+2}{2} \rfloor} b_{2j+1}$ es par.

De esta manera el teorema 1.17 implica que $D_{k+2}(x,1)$ es un polinomio de permutación módulo $n = 2^\omega$ con $\omega \geq 2$, como se afirma. □

2.8. Polinomios de Dickson módulo n

En esta sección se presentan algunos resultados de polinomios de Dickson sobre el anillo $\mathbb{Z}_n$, donde $n = \prod_{i=1}^{r} p_i^{e_i}$, con los p_i primos distintos, para $1 \leq i \leq r$ (cf. [13]). Además se demuestran resultados importantes para determinar si un polinomio de Dickson es un polinomio de permutación de $\mathbb{Z}_n$.

Escribimos $[a_1, a_2, \ldots, a_r]$ para el mínimo común múltiplo y $(a_1, a_2, \ldots, a_r)$ para el máximo común divisor de los enteros $a_1, a_2, \ldots, a_r$. Con esta notación se define

$$v(n) = \left[p_1^{e_1-1}(p_1^2 - 1), \ldots, p_r^{e_r-1}(p_r^2 - 1)\right] \tag{2.30}$$

De manera similar a la definición 1, un polinomio $f(x) \in \mathbb{Z}[x]$ es llamado polinomio de permutación de $\mathbb{Z}_n$ ó polinomio de permutación mód n, si la función asociada $f : c \to f(c)$ de $\mathbb{Z}_n$ a $\mathbb{Z}_n$ es una permutación de $\mathbb{Z}_n$, es decir, es una función biyectiva de $\mathbb{Z}_n$ en sí mismo.

Primero consideramos algunas propiedades generales de los polinomios de permutación de $\mathbb{Z}_n$.

Definición 3. *Sea $r(x) = \frac{g(x)}{h(x)}$ un cociente de polinomios primos sobre $\mathbb{Z}$. Entonces $r(x)$ es llamada una* ***función de permutación mód*** *n si $h(i)$ mód n y n son primos relativos para cada $i \in \mathbb{Z}$ y la función asociada $r(i) \equiv h(i)^{-1}g(i)$ (mód n), con $1 \leq i \leq n$, es una permutación módulo n.*

Notemos que $g(x)$ es un polinomio de permutación mód n si y sólo si es una permutación de $\mathbb{Z}_n$, y esto sucede si y sólo si $\frac{g(x)}{1}$ es una función de permutación mód n.

Lema 2.8. *El cociente de polinomios $r(x) = \frac{g(x)}{h(x)}$ es una función de permutación módulo n si y sólo si $h(i)$ mód n y n son primos relativos para todo $i \in \mathbb{Z}$ y la congruencia $g(x) - \lambda h(x) \equiv 0$ (mód n) es soluble en $\mathbb{Z}_n$ para cada entero λ.*

Demostración. Supóngase primero que $r(x)$ es una función de permutación mód n, entonces por la definición 3, se tiene que $mcd(h(i) \text{ mód } n,\ n) = 1$ para $i \in \mathbb{Z}$ y la función asociada $r(i) \equiv h(i)^{-1}g(i)$ (mód n), con $1 \leq i \leq n$, es una permutación mód n.

Considere $\lambda \in \mathbb{Z}$, la congruencia $g(x) - \lambda h(x) \equiv 0$ (mód n) y $v = \lambda$ mód n, es decir $v \equiv \lambda$ (mód n) y $0 \leq v < n$. Como se está suponiendo que $r(i) \equiv h(i)^{-1}g(i)$ (mód n), con $i = 1, 2, \ldots, n$ es una permutación mód n, entonces existe i tal que $1 \leq i \leq n$ y $v \equiv r(i)$ (mód n), por lo que una solución de $g(x) - \lambda h(x) \equiv 0$ (mód n) es i pues $\lambda \equiv h(i)^{-1}g(i)$ (mód n).

Recíprocamente supóngase que $mcd(h(i) \text{ mód } n,\ n) = 1$ para todo $i \in \mathbb{Z}$ y que la congruencia $g(x) - \lambda h(x) \equiv 0$ (mód n) es soluble para cada entero λ. Entonces para cada $\lambda \in \mathbb{Z}$ existe $i \in \mathbb{Z}_n$ tal que $g(i) - \lambda h(i) \equiv 0$ (mód n) y como $mcd(h(i) \text{ mód } n,\ n) = 1$ para todo $i \in \mathbb{Z}$, se puede despejar a λ y se obtiene $\lambda \equiv h(i)^{-1}g(i)$ (mód n), de esta manera $r(i) \equiv \lambda$ (mód n).

Por lo tanto para cada $\lambda \in \mathbb{Z}$ existe $i \in \mathbb{Z}_n$ tal que $r(i) \equiv \lambda$ (mód n), por lo que $r(i)$ es una permutación mód n. □

Lema 2.9. *Si $n = ab$, donde $mcd(a, b) = 1$, entonces $r(x) = \frac{g(x)}{h(x)}$ es una función de permutación mód n si y sólo si $r(x)$ es una función de permutación mód a y mód b.*

Demostración. Si $r(x)$ es una función de permutación mód n, entonces por el lema 2.8 esto sucede si y sólo si la congruencia $g(x) - \lambda h(x) \equiv 0$ (mód n) tiene solución para toda $\lambda \in \mathbb{Z}$. Por lo que se tiene el siguiente sistema de congruencias

$$g(x) - \lambda h(x) \equiv 0 \text{ (mód } a) \text{ y } g(x) - \lambda h(x) \equiv 0 \text{ (mód } b)$$

Por hipótesis $mcd(a, b) = 1$, así que el Teorema Chino del Residuo implica la existencia de una solución única al sistema, para cada $\lambda \in \mathbb{Z}$, por lo tanto $r(x)$ es una función de permutación mód a y mód b.

Así $r(x) = \frac{g(x)}{h(x)}$ es una función de permutación mód n si y sólo si $r(x)$ es una función de permutación mód a y mód b. □

Considerando $h(x) = 1$ en el lema anterior se tiene que $r(x) = g(x)$, y de esta manera $g(x)$ es un polinomio de permutación mód n si y sólo si $g(x)$ es un polinomio de permutación mód a y mód b.

Por lo tanto podemos reducir el estudio de las funciones de permutación mód n (o polinomios de permutación mód n) a los polinomios de permutación mód p^e, donde p es un primo y $e \geq 1$ es un entero. Este caso se tiene con el siguiente lema:

Lema 2.10. *El cociente $r(x) = \frac{g(x)}{h(x)}$ es una función de permutación mód p^e, $e > 1$ si y sólo si es una función de permutación mód p y $h(i)g'(i) - g(i)h'(i) \not\equiv 0$ (mód p) para todo $i \in \mathbb{Z}_p$.*

Demostración. Se tiene que la derivada de $r(x)$ es: $r'(x) = \frac{h(x)g'(x) - g(x)h'(x)}{h^2(x)}$.

Por el corolario 1.16 se cumple que $r(x)$ es función de permutación mód p^e, $e > 1$ si y sólo si $r(x)$ es función de permutación mód p y además $r'(i) \not\equiv 0 \pmod{p}$ para todo $i \in \mathbb{Z}_p$, esto último es equivalente a $h(i)g'(i) - g(i)h'(i) \not\equiv 0 \pmod{p}$ para todo $i \in \mathbb{Z}_p$. □

Teorema 2.11.

- *Si n no es libre de cuadrados, entonces el único polinomio de permutación mód n de la forma x^m es x.*
- *Si $n = \prod_{i=1}^{r} p_i$, donde los p_i son primos distintos, entonces x^m es polinomio de permutación mód n si y sólo si $(n, [p_1 - 1, \ldots, p_r - 1]) = 1$.*

Demostración. Si n no es libre de cuadrados sería de la forma $n = p^{2e}b$, con p primo, $e \geq 1$ y $b \in \mathbb{Z}$ tal que $(p, b) = 1$. Si $g(x) = x^m$ es un polinomio de permutación mód n por el lema 2.9 también sería un polinomio de permutación mód p^e y como una consecuencia del lema 2.10 se tiene $g'(x) \not\equiv 0 \pmod{p}$, pero $g'(x) = mx^{m-1}$ y $mx^{m-1} \not\equiv 0 \pmod{p}$ si y sólo si $m = 1$. Por lo tanto el único polinomio de permutación mód n de la forma x^m es x.

Para demostrar la segunda parte del teorema, se hará inducción sobre r

Si $r = 2$, entonces por el lema 2.9 $g(x) = x^m$ es polinomio de permutación mód n donde $n = p_1p_2$ con $(p_1, p_2) = 1$ si y sólo si $g(x)$ es polinomio de permutación mód p_1 y mód p_2, por el teorema 1.8 esto sucede si y sólo si $(m, p_1 - 1) = 1$ y $(m, p_2 - 1) = 1$ lo que equivale a

$$(m, (p_1 - 1)(p_2 - 1)) = 1.$$

Además $[p_1 - 1, p_2 - 1] | (p_1 - 1)(p_2 - 1)$, por lo que $(m, (p_1 - 1)(p_2 - 1)) = 1$ si y sólo si $(m, [p_1 - 1, p_2 - 1]) = 1$.

Supóngase que la proposición se cumple para $r = k$. Sea $n = \prod_{i=1}^{k+1} p_i$ y considere $n' = \frac{n}{p_{k+1}}$. Por el lema 2.9 $g(x) = x^m$ es polinomio de permutación mód n si y sólo si es polinomio de permutación mód n' y mód p_{k+1}. Por el teorema 1.8 $g(x)$ es polinomio de permutación mód p_{k+1} si y sólo si $(m, p_{k+1} - 1) = 1$. Y por la hipótesis de inducción $g(x)$ es polinomio de permutación mód n' si y sólo si $(m, [p_1 - 1, p_2 - 1, \ldots, p_k - 1]) = 1$. Pero $(m, p_{k+1} - 1) = 1$ y $(m, [p_1 - 1, p_2 - 1, \ldots, p_k - 1]) = 1$ si y sólo si

$$(m, (p_{k+1} - 1)\,[p_1 - 1, p_2 - 1, \ldots, p_k - 1]) = 1,$$

y como

$$[p_1 - 1, p_2 - 1, \ldots, p_k - 1, p_{k+1} - 1] \,|(p_{k+1} - 1)\,[p_1 - 1, p_2 - 1, \ldots, p_k - 1]$$

se tiene que $(m, (p_{k+1} - 1)\,[p_1 - 1, p_2 - 1, \ldots, p_k - 1]) = 1$ o equivalentemente que

$$(m, [p_1 - 1, p_2 - 1, \ldots, p_{k+1} - 1]) = 1.$$

De esta manera $g(x)$ es polinomio de permutación mód n si y sólo si

$$(m, [p_1 - 1, p_2 - 1, \ldots, p_{k+1} - 1]) = 1.$$

□

Teorema 2.12. *El polinomio de Dickson de gardo k, $D_k(x, a)$ con $a \in \mathbb{Z}_n$, $a \neq 0$ y $(a, n) = 1$, es un polinomio de permutación mód n si y sólo si $(k, v(n)) = 1$, donde $v(n)$ es como en (2.30).*

Demostración. Se procede realizando inducción con r.

Si $r = 1$, entonces $n = p_1^{e_1}$ y por hipótesis $(a, p_1^{e_1}) = 1$. Por el corolario 1.16 $D_k(x, a)$ es polinomio de permutación mód $p_1^{e_1}$ si y sólo si $D_k(x, a)$ es polinomio de permutación mód p_1 y $D'_k(x, s) \not\equiv 0$ (mód p_1) para cada entero s, y por el teorema 2.4 esto equivale a la condición $(k, p_1) = 1$. Además como consecuencia del teorema 2.3 se tiene que $D_k(x, a)$ es polinomio de permutación mód p_1 si y sólo si $(k, p_1^2 - 1) = 1$. Por lo tanto $(k, p_1^{e_1}) = 1$ y así $D_k(x, a)$ es polinomio de permutación mód $p_1^{e_1}$ si y sólo si $(k, p_1^{e_1}(p_1^2 - 1)) = 1$.

Ahora si $r = 2$, se tiene que $n = p_1^{e_1} p_2^{e_2}$, $(a, n) = 1$, $(p_1^{e_1}, p_2^{e_2}) = 1$. Por el lema 2.9 $D_k(x, a)$ es polinomio de permutación mód n es equivalente a que $D_k(x, a)$ es polinomio de permutación mód $p_1^{e_1}$ y mód $p_2^{e_2}$, y por el caso $r = 1$ esto se tiene si y sólo si $(k, p_1^{e_1}(p^2{}_1 - 1)) = 1$ y $(k, p_2^{e_2}(p^2{}_2 - 1)) = 1$ es decir $(k, v(n)) = 1$.

Supóngase que para $r = t$ se cumple el teorema, $n = \prod_{i=1}^{t+1} p_i^{e_i}$ el producto de primos distintos y definamos $n' = \prod_{i=1}^{t} p_i^{e_i}$. Por hipótesis de inducción, $D_k(x, a)$ es polinomio de permutación mód n' si y sólo si $(k, v(n')) = 1$. Además $D_k(x, a)$ es polinomio de permutación mód n si y sólo si $D_k(x, a)$ es polinomio de permutación mód n' y mód $p_{t+1}^{e_{t+1}}$, por el caso $r = 2$ esto sucede si y sólo si $(k, v(n)) = 1$. □

Como caso particular para $a = 1$, denotaremos $D_k(x, 1) = D_k(x)$, que es polinomio de permutación mód n si y sólo si $(k, v(n)) = 1$.

Siguiendo con los polinomios de permutación módulo 2^ω, como consecuencia del teorema 2.12 el polinomio de Dickson de grado k, $D_k(x)$, es un polinomio de permutación módulo 2^ω si y sólo si $(k, 3 \cdot 2^\omega) = 1$, lo que es equivalente a que k debe ser impar y no es múltiplo de 3, esto contradice un resultado que en [28] dice que $D_k(x)$ es un polinomio de permutación módulo 2^ω si y sólo si k es impar, un contraejemplo es $D_9(x)$ como se mostró en el ejemplo 5.

Capítulo 3

Polinomios de permutación de Dickson

Este capítulo contiene los resultados necesarios para justificar el sistema de cifrado basado en polinomios de Dickson que se presenta en el siguiente capítulo. Se demuestra bajo qué condiciones existe la inversa de los polinomios de permutación de Dickson, y esto permite que al cifrar un mensaje siempre sea posible descifrarlo. Los resultados se encuentran en [11].

Definición 4. *Definimos el conjunto de polinomios de permutación de Dickson mód n como:*

$$D(n) = \{D_k(x) : D_k(x) \text{ es un polinomio de permutación mód } n\}.$$

Lema 3.1. *$D(n)$ es un semigrupo abeliano bajo la composición.*

Demostración. Sean $D_k(x), D_l(x) \in D(n)$ y π, ρ las permutaciones inducidas por $D_k(x)$ y $D_l(x)$, respectivamente. Así $\pi \circ \rho$ es inducida por $D_k(x) \circ D_l(x)$.

Por el inciso (2) del lema 2.2 se tiene que $D_{kl}(x,1) = D_k(D_l(x,1),1)$, por lo que $D_{kl}(x) = D_k(D_l(x))$. Por lo tanto la permutación $\pi \circ \rho$ es inducida por $D_{kl}(x)$.

Ahora sean $D_k(x), D_l(x), D_m(x) \in D(n)$, entonces

$$\begin{aligned}[D_k(x) \circ D_l(x)] \circ D_m(x) &= D_{kl}(x) \circ D_m(x) = D_{klm}(x) \\ &= D_k(x) \circ D_{lm}(x) = D_k(x) \circ [D_l(x) \circ D_m(x)].\end{aligned}$$

Así $D(n)$ es un semigrupo bajo la composición. Y como

$$D_k(x) \circ D_l(x) = D_{kl}(x) = D_{lk}(x) = D_l(x) \circ D_k(x)$$

$D(n)$ es conmutativo bajo la composición. □

Notemos que $D_1(x) = x$ es la permutación identidad módulo n y por lo tanto es invertible. Enseguida se muestran resultados que nos permiten justificar la existencia de la inversa de un polinomio de permutación de Dickson. Se define G_n como el conjunto de permutaciones π sobre $\mathbb{Z}_n$ para las que existe un polinomio de Dickson $D_k(x) \in D(n)$ con $\pi(a \mod n) = D_k(a) \mod n$, esto para toda $a \in \mathbb{Z}$.

Si π es una permutación inducida por el polinomio de permutación de Dickson $D_k(x)$ mód n, entonces por el teorema 2.12 se tiene que $(k, v(n)) = 1$ por lo que existe $l \in \mathbb{Z}^*_{v(n)}$ tal que $kl \equiv 1 \pmod{v(n)}$, y así $(l, v(n)) = 1$ y por el teorema 2.12 $D_l(x)$ es un polinomio de permutación mód n. Sólo nos falta ver que efectivamente $D_{kl}(x) \equiv D_1(x) \pmod{n}$. Resultados que nos ayudan a demostrarlo se encuentran en [11], en donde se abordan 3 casos diferentes para G_n analizados en las siguientes secciones.

El objetivo final es dar algunos resultados sobre la cardinalidad de G_n y probar que es un grupo.

3.1. G_{p^e} para $p \geq 5$

En esta sección iniciamos el estudio de G_n, con n una potencia de un primo dado p.

Lema 3.2. *Existe una extensión de $\mathbb{Z}_{p^2}$ donde la ecuación $(y \pm 1)^2 = (p\lambda)y$, con $\lambda \in \mathbb{Z}_{p^2}$, tiene una solución η con $\eta^{2p} = 1$.*

Demostración. Sean $J = \langle (y \pm 1)^2 - (p\lambda)y, p(y \pm 1) \rangle$ un ideal de $\mathbb{Z}_{p^2}[x]$ y considere el anillo $R = \mathbb{Z}_{p^2}[y]/J$. Se define la función $\varphi : \mathbb{Z}_{p^2} \to R$ como $\varphi(a) = a + J$, que es un morfismo pues para $a, b \in \mathbb{Z}_{p^2}$ se tiene:

$$\varphi(a + b) = (a + b) + J = (a + J) + (b + J) = \varphi(a) + \varphi(b).$$

Analicemos el núcleo de φ, que denotamos como $Nu(\varphi)$:

$$\begin{aligned} a \in Nu(\varphi) &\Leftrightarrow \varphi(a) = J \text{ en } R \Leftrightarrow a + J = J \text{ en } R \Leftrightarrow a \in J \text{ en } \mathbb{Z}_{p^2}[y] \\ &\Leftrightarrow a = u(y)\left[(y \pm 1)^2 - (p\lambda)y\right] + v(y)\left[p(y \pm 1)\right], \text{ en } \mathbb{Z}_{p^2}[y] \\ &\quad \text{con } u(y), v(y) \in \mathbb{Z}_{p^2}[y] \\ &\Leftrightarrow a = u(y)\left[(y \pm 1)^2 - (p\lambda)y\right] + v(y)\left[p(y \pm 1)\right] + p^2 w(y), \\ &\quad \text{en } \mathbb{Z}[y], \text{ con } w(y) \in \mathbb{Z}[y] \end{aligned}$$

Ahora si reducimos módulo p la última igualdad se tiene que

$$a \equiv u(y)(y \pm 1)^2 \pmod{p}$$

Sea $u(y) = \sum_{i=0}^{n} u_i y^i$, así

$$\begin{aligned} u(y)(y \pm 1)^2 &= (y^2 \pm 2y + 1) \sum_{i=0}^{n} u_i y^i = \sum_{i=0}^{n} u_i y^{i+2} \pm 2 \sum_{i=0}^{n} u_i y^{i+1} + \sum_{i=0}^{n} u_i y^i \\ &= \sum_{i=2}^{n+2} u_{i-2} y^i \pm 2 \sum_{i=1}^{n+1} u_{i-1} y^i + \sum_{i=0}^{n} u_i y^i \end{aligned}$$

como a es constante, entonces

$$\begin{aligned} a &= u_0 \\ 0 &= \pm 2u_0 + u_1 \\ 0 &= u_{i-2} \pm 2u_{i-1} + u_i, \text{ con } 2 \leq i \leq n \\ 0 &= u_{n-1} \pm 2u_n \\ 0 &= u_n \end{aligned}$$

de donde $u_{n-1} = 0$ y resolviendo de forma recursiva

$$u_{i-2} = -u_i \mp 2u_{i-1}, \text{ con } 2 \leq i \leq n$$

en el cual $u_{i-2} = 0$ para $2 \leq i \leq n$, así $u_0 = 0$ y por lo tanto $u(y) \equiv 0 \pmod{p}$.

Se encuentra $a \equiv 0 \pmod{p}$. Entonces $a = p\alpha,\ \alpha \in \mathbb{Z}$ y $u(y) = pu_1(y)$ con $u_1(y) \in \mathbb{Z}[y]$, luego

$$p\alpha = pu_1(y)\left[(y \pm 1)^2 - (p\lambda)y\right] + v(y)\left[p(y \pm 1)\right] + p^2 w(y) \text{ en } \mathbb{Z}[y]$$

primero, al dividir entre p se obtiene

$$\alpha = u_1(y)\left[(y \pm 1)^2 - (p\lambda)y\right] + v(y)(y \pm 1) + pw(y)$$

a continuación, se reduce módulo p y resulta

$$\alpha \equiv u_1(y)(y \pm 1)^2 + v(y)(y \pm 1) \pmod{p}.$$

La congruencia se cumple para cualquier valor de y, en particular para $y = \mp 1$ y así tenemos $\alpha \equiv 0 \pmod{p}$, por lo que $a \equiv 0 \pmod{p^2}$.

Por lo tanto $Nu(\varphi) = \{0\}$. Como φ es inyectiva R es una extensión del anillo $\mathbb{Z}_{p^2}$.

Sea η la clase de residuos de y en R, entonces $(\eta \pm 1)^2 - (p\lambda)\eta = 0$ y $p(\eta \pm 1) = 0$, por lo tanto

$$\begin{aligned} \eta^{2p} &= \left[((\eta \pm 1) \mp 1)^p\right]^2 = \left[\sum_{i=0}^{p} \binom{p}{i} (\eta \pm 1)^{p-i} (\mp 1)^i\right]^2 \\ &= \left[(\eta \pm 1)^p + p \sum_{i=0}^{p-1} \binom{p-1}{i} (\eta \pm 1)^{p-i} (\mp 1)^i + (\mp 1)\right]^2 \\ &= \left[(\eta \pm 1)^p + p(\eta \pm 1) \sum_{i=0}^{p-1} \binom{p-1}{i} (\eta \pm 1)^{p-1-i} (\mp 1)^i + (\mp 1)\right]^2 \\ &= \left[(\eta \pm 1)^2 (\eta \pm 1)(\eta \pm 1)^{p-3} \mp 1\right]^2 = \left[\lambda\eta p(\eta \pm 1)(\eta \pm 1)^{p-3} \mp 1\right]^2 = (\mp 1)^2 = 1. \end{aligned}$$

□

Lema 3.3. *Sea $u \in \mathbb{Z}$ con $u \not\equiv \pm 2 \pmod{p}, p > 2$ y $e \geq 1$. Entonces existen $h_1(y), h_2(y) \in \mathbb{Z}[y]$ tales que*

$$y^{p^{e-1}\frac{p^2-1}{2}} = 1 + h_1(y)(y^2 - uy + 1) + p^e h_2(y)$$

Demostración. Haciendo inducción sobre e.

Si $e = 1$, considere η una solución de la ecuación

$$y^2 - uy + 1 = 0 \tag{3.1}$$

definida sobre $\mathbb{Z}_p$. Entonces se tienen 2 posibilidades: $\eta \in \mathbb{Z}_p$ ó $\eta \notin \mathbb{Z}_p$.

- Supóngase que $\eta \in \mathbb{Z}_p$ y notemos que $\eta \neq 0$ pues si $\eta = 0$ se tendría $1 = 0$ lo que no puede ser. Como $u \not\equiv \pm 2$ (mód p), entonces

  $$y^2 - uy + 1 \not\equiv (y \pm 1)^2 \text{ (mód } p)$$

  por lo que $\eta \neq \pm 1$.

  Así $\eta^{p-1} = 1$, por lo tanto $\eta^{\frac{p^2-1}{2}} = \eta^{(p-1)\frac{p+1}{2}} = 1$, además existe $\eta^{-1} \in \mathbb{Z}_p$, y por ser η solución de (3.1) $\eta^2 - u\eta + 1 = 0$. Al multiplicar por η^{-2} se obtiene

  $$1 - \frac{u}{\eta} + \frac{1}{\eta^2} = 0,$$

  entonces

  $$(\eta^{-1})^2 - u(\eta^{-1}) + 1 = 0$$

  y $\eta \neq \eta^{-1}$ debido a que $u \not\equiv \pm 2$ (mód p). En consecuencia η^{-1} es la otra raíz de (3.1).

  Así $y^2 - uy + 1 = (y - \eta)(y - \eta^{-1})$, por lo que todo cero de $y^2 - uy + 1 = 0$ es un cero de $y^{\frac{p^2-1}{2}} - 1 = 0$, lo que implica que $(y^2 - uy + 1) \mid \left(y^{\frac{p^2-1}{2}} - 1\right)$.

- Ahora si $\eta \notin \mathbb{Z}_p$, entonces $y^2 - uy + 1$ es irreducible sobre $\mathbb{Z}_p$, $\eta^2 - u\eta + 1 = 0$. Elevando a la potencia p se tiene

  $$(\eta^2 - u\eta + 1)^p = (\eta^p)^2 - u^p\eta^p + 1 = (\eta^p)^2 - u(\eta^p) + 1 = 0,$$

  de donde η y η^p son soluciones de (3.1), pero sus únicas soluciones son η y η^{-1}, de manera que $\eta^p = \eta^{-1}$.

  La última igualdad implica que $\eta^{p+1} = 1$. Así $\eta^{\frac{p^2-1}{2}} = \eta^{(p+1)\frac{p-1}{2}} = 1$. Luego como antes, se cumple que $(y^2 - uy + 1) \mid \left(y^{\frac{p^2-1}{2}} - 1\right)$.

En cualquier caso se tiene $(y^2 - uy + 1) \mid \left(y^{\frac{p^2-1}{2}} - 1\right)$, por tal motivo existe el polinomio $h_1(y) \in \mathbb{Z}_p[y]$ tal que

$$y^{\frac{p^2-1}{2}} - 1 = h_1(y)(y^2 - uy + 1) \text{ en } \mathbb{Z}_p[y].$$

Se sigue que existe $h_2(y) \in \mathbb{Z}[y]$ tal que

$$y^{\frac{p^2-1}{2}} = 1 + h_1(y)(y^2 - uy + 1) + ph_2(y) \text{ en } \mathbb{Z}[y].$$

Supóngase que el lema se cumple para $e = k - 1$. Queremos calcular $y^{p^{k-1}\frac{p^2-1}{2}}$, que reescribimos como

$$y^{p^{k-1}\frac{p^2-1}{2}} = \left[y^{p^{k-2}\frac{p^2-1}{2}}\right]^p.$$

Por hipótesis de inducción existen $\overline{h_1}(y), \overline{h_2}(y) \in \mathbb{Z}[y]$ tales que

$$y^{p^{k-2}\frac{p^2-1}{2}} = 1 + \overline{h_1}(y)(y^2 - uy + 1) + p^{k-1}\overline{h_2}(y)$$

de este modo

$$\begin{aligned} y^{p^{k-1}\frac{p^2-1}{2}} &= \left[1 + \overline{h_1}(y)(y^2 - uy + 1) + p^{k-1}\overline{h_2}(y)\right]^p \\ &= \sum_{i=0}^{p} \binom{p}{i} \left[1 + p^{k-1}\overline{h_2}(y)\right]^{p-i} \left[\overline{h_1}(y)(y^2 - uy + 1)\right]^i \end{aligned}$$

representando como $h_1(y)$:

$$\overline{h_1}(y) \sum_{i=1}^{p} \binom{p}{i} \left[1 + p^{k-1}\overline{h_2}(y)\right]^{p-i} \left[\overline{h_1}(y)(y^2 - uy + 1)\right]^{i-1}$$

se obtiene

$$\begin{aligned} y^{p^{k-1}\frac{p^2-1}{2}} &= \sum_{i=0}^{p} \binom{p}{i} \left[p^{k-1}\overline{h_2}(y)\right]^i + h_1(y)(y^2 - uy + 1) \\ &= 1 + p(p^{k-1}\overline{h_2}(y)) + p^k \sum_{i=2}^{p} \binom{p}{i} p^{k-2} \left[p^{k-1}\overline{h_2}(y)\right]^{i-2} \overline{h_2^2}(y) + h_1(y)(y^2 - uy + 1) \end{aligned}$$

haciendo $h_2(y) = \overline{h_2}(y) + \sum_{i=2}^{p} \binom{p}{i} p^{k-2} \left[p^{k-1}\overline{h_2}(y)\right]^{i-2} \overline{h_2^2}(y)$ se tiene la igualdad

$$y^{p^{k-1}\frac{p^2-1}{2}} = 1 + h_1(y)(y^2 - uy + 1) + p^k h_2(y)$$

como se deseaba. □

Corolario 3.4. *Sea $p > 2$ primo, $e \geq 1$. Para cada $u \in \mathbb{Z}_{p^e}$ la ecuación $y^2 - uy + 1 = 0$ tiene una raíz de η con $\eta^{p^{e-1}\cdot\frac{p^2-1}{2}} = 1$ en una extensión de $\mathbb{Z}_{p^e}$.*

Demostración. Si $u \not\equiv \pm 2 \pmod{p}$, entonces por el lema 3.3 existen $h_1(y), h_2(y) \in \mathbb{Z}[y]$ tales que

$$y^{p^{e-1}\frac{p^2-1}{2}} = 1 + h_1(y)(y^2 - uy + 1) + p^e h_2(y)$$

por lo que $y^{p^{e-1}\frac{p^2-1}{2}} = 1$ en $\mathbb{Z}_{p^e}[y]/\langle y^2 - uy + 1\rangle$.

Sea η una raíz de $y^2 - uy + 1 = 0$, así tenemos que $\eta \in \mathbb{Z}_{p^e}[y]/\langle y^2 - uy + 1\rangle$ y por lo tanto $\eta^{p^{e-1}\cdot\frac{p^2-1}{2}} = 1$.

Supóngase ahora que $u \equiv \pm 2 \pmod{p}$, es decir $u = \pm 2 + p\lambda$, $\lambda \in \mathbb{Z}$ de donde $y^2 - uy + 1 = y^2 - (\pm 2 + p\lambda)y + 1 = 0$ si y sólo si $y^2 \mp 2y + 1 = p\lambda y$, lo que es equivalente a $(y \mp 1)^2 = p\lambda y$.

Para demostrar el corolario en este caso se usará inducción sobre e.

Cuando $e = 1$, notemos que la ecuación $y^2 - uy + 1 = 0$ es equivalente a $(y \pm 1)^2 \equiv 0 \pmod{p}$, lo que se cumple si y sólo si $y = \mp 1 \bmod p$.

Así que la raíz de $y^2 - uy + 1 = 0$ en $\mathbb{Z}_p$ es $\eta = \mp 1$.

Como p es primo impar, entonces $p = 2t + 1$ para algún entero t, y así

$$\frac{p^2 - 1}{2} = \frac{(2t+1)^2 - 1}{2} = \frac{4t^2 + 4t + 1 - 1}{2} = 2(t^2 + t)$$

es par, por lo tanto $\eta^{\frac{p^2-1}{2}} = (\mp 1)^{2(t^2+t)} = 1$.

Si $e = 2$, por el lema 3.2 existe η en una extensión de $\mathbb{Z}_{p^2}$ tal que $\eta^{2p} = 1$, y como $\frac{p^2-1}{2}$ es par, entonces $\frac{p^2-1}{2} = 2s$ con $s \in \mathbb{Z}$ y de esta manera $\eta^{p\frac{p^2-1}{2}} = \eta^{2ps} = 1$.

Al ser todos los ceros de $y^2 - uy + 1 = 0$ ceros de $y^{p\frac{p^2-1}{2}} - 1 = 0$, se sigue que

$$(y^2 - uy + 1) | (y^{p\frac{p^2-1}{2}} - 1) \text{ en } \mathbb{Z}_{p^e}[y]/\left\langle y^2 - uy + 1, p(y \pm 1)\right\rangle$$

de donde existen $u(y), v(y), w(y) \in \mathbb{Z}[y]$ tales que

$$y^{p\frac{p^2-1}{2}} = 1 + u(y)(y^2 - uy + 1) + v(y)p(y \pm 1) + p^2 w(y).$$

Supóngase que el corolario se cumple para $e = k$, siguiendo con la idea del caso $e = 2$ se tiene que

$$y^{p^{k-1}\frac{p^2-1}{2}} = 1 + \bar{u_1}(y)(y^2 - uy + 1) + \bar{v}(y)p(y \pm 1) + p^k \bar{w}(y) \tag{3.2}$$

con $\bar{u_1}(y), \bar{v}(y)$ y $\bar{w}(y)$ en $\mathbb{Z}[y]$.

Sea $e = k + 1$, nótese que si se demuestra que

$$y^{p^k\frac{p^2-1}{2}} = 1 + u_1(y)(y^2 - uy + 1) + v(y)p(y \pm 1) + p^{k+1} w(y) \tag{3.3}$$

con $u_1(y), v(y), w(y)$ en $\mathbb{Z}[y]$, se tendría que

$$y^{p^k \frac{p^2-1}{2}} = 1 \text{ en } \mathbb{Z}_{p^{k+1}}[y]/\left\langle y^2 - uy + 1, p(y \pm 1)\right\rangle.$$

De este modo η resultaría ser una raíz de $y^2 - uy + 1 = 0$ en la extensión $\mathbb{Z}_{p^{k+1}}[y]/\left\langle y^2 - uy + 1, p(y \pm 1)\right\rangle$ y así $\eta^{p^k \frac{p^2-1}{2}} = 1$.

Para demostrar (3.3) elevamos a la potencia p la igualdad (3.2) y se obtiene:

$$\begin{aligned} y^{p^k \frac{p^2-1}{2}} &= \left[y^{p^{k-1} \frac{p^2-1}{2}}\right]^p = \left[1 + \bar{u}(y)(y^2 - uy + 1) + \bar{v}(y)p(y \pm 1) + p^k \bar{w}(y)\right] \\ &= \sum_{i=0}^{p} \binom{p}{i} \left[\bar{u}(y)(y^2 - uy + 1)\right]^{p-i} \left[1 + \bar{v}(y)p(y \pm 1) + p^k \bar{w}(y)\right]^i, \end{aligned}$$

si $u(y) = \sum_{i=0}^{p-1} \binom{p}{i} (\bar{u}(y))^{p-i} (y^2 - uy + 1)^{p-1-i} \left[1 + \bar{v}(y)p(y \pm 1) + p^k \bar{w}(y)\right]^i$,

$$\begin{aligned} y^{p^k \frac{p^2-1}{2}} &= u(y)(y^2 - uy + 1) + \left[1 + \bar{v}(y)p(y \pm 1) + p^k \bar{w}(y)\right]^p \\ &= u(y)(y^2 - uy + 1) + \sum_{i=0}^{p} \binom{p}{i} \left[1 + p^k \bar{w}(y)\right]^{p-i} \left[\bar{v}(y)p(y \pm 1)\right]^i. \end{aligned}$$

haciendo $v(y) = \sum_{i=1}^{p} \binom{p}{i} \left[1 + p^k \bar{w}(y)\right]^{p-i} (\bar{v}(y))^i \left[p(y \pm 1)\right]^{i-1}$ se obtiene

$$y^{p^k \frac{p^2-1}{2}} = u(y)(y^2 - uy + 1) + v(y)p(y \pm 1) + \left[1 + p^k \bar{w}(y)\right]^p$$

el último sumando puede desarrollarse como:

$$\left[1 + p^k \bar{w}(y)\right]^p = \sum_{i=0}^{p} \binom{p}{i} \left[p^k \bar{w}(y)\right]^i = 1 + p\left[p^k \bar{w}(y)\right] + \sum_{i=2}^{p} \binom{p}{i} \left[p^k \bar{w}(y)\right]^2 \left[p^k \bar{w}(y)\right]^{i-2}$$

al hacer la sustitución $w(y) = \bar{w}(y) + \sum_{i=2}^{p} \binom{p}{i} p^{k-1} (\bar{w}(y))^2 \left[p^k \bar{w}(y)\right]^{i-2}$, resulta

$$y^{p^k \frac{p^2-1}{2}} = u(y)(y^2 - uy + 1) + v(y)p(y \pm 1) + p^{k+1} w(y),$$

con lo que se concluye la demostración.

□

Teorema 3.5. *Sea p primo impar y $k, l \in \mathbb{N}$ tales que $k \equiv l \pmod{p^{e-1}\left(\frac{p^2-1}{2}\right)}$. Entonces*

$$D_k(v) \equiv D_l(v) \pmod{p^e} \text{ para todo } v \in \mathbb{Z}.$$

Demostración. Sea $v \in \mathbb{Z}$ y suponga que $u = v$ mód p^e. Por el corolario 3.4 la ecuación $y^2 - uy + 1 = 0$ tiene una raíz η con $\eta^{p^{e-1}\frac{p^2-1}{2}} = 1$ en una extensión de $\mathbb{Z}_{p^e}$, sea R tal extensión, así η es una raíz de la unidad en R.

Además $u = \eta + \eta^{-1}$ pues $\eta(\eta + v) = 1$. Se está suponiendo que se cumple la congruencia $k \equiv l \pmod{p^{e-1}\left(\frac{p^2-1}{2}\right)}$, entonces existe $s \in \mathbb{Z}$ tal que $k = l + sp^{e-1}\left(\frac{p^2-1}{2}\right)$.

Así

$$\begin{aligned} D_k(u) &= D_k(\eta + \eta^{-1}) \equiv \eta^k + \eta^{-k} \pmod{p^e} \\ &\equiv \eta^l \eta^{sp^{e-1}\left(\frac{p^2-1}{2}\right)} + \eta^{-l}\eta^{-sp^{e-1}\left(\frac{p^2-1}{2}\right)} \pmod{p^e} \equiv \eta^l + \eta^{-l} \pmod{p^e} \\ &\equiv D_l(\eta + \eta^{-1}) \pmod{p^e} \equiv D_l(u) \pmod{p^e} \end{aligned}$$

Como $D_k(v) \equiv D_k(u) \pmod{p^e}$ y $D_l(v) \equiv D_l(u) \pmod{p^e}$, entonces para cada $v \in \mathbb{Z}$ se tiene que $D_k(v) \equiv D_l(v) \pmod{p^e}$.

□

Corolario 3.6. *Sea p un primo impar. Para cada $u \in \mathbb{Z}_{p^e}$, definimos:*

$$\psi : \mathbb{Z}^*_{p^{e-1}\left(\frac{p^2-1}{2}\right)} \to G_{p^e}$$

$$\psi(k) = D_k(u)$$

Entonces ψ es un epimorfismo.

Demostración. Sean $k, l \in \mathbb{Z}^*_{p^{e-1}\left(\frac{p^2-1}{2}\right)}$ y $u \in \mathbb{Z}^*_{p^e}$ arbitrario, se tiene

$$\psi(kl) = D_{kl}(u) = D_k(D_l(u)) = D_k(u) \circ D_l(u) = \psi(k) \circ \psi(l).$$

Por lo tanto ψ es un morfismo.

Sea $D_k(x) \in G_{p^e}$, de donde $D_k(x)$ es un polinomio de permutación mód p^e, y por el teorema 2.12 esto sucede si y sólo si $(k, p^{e-1}(p^2-1)) = 1$ lo que equivale a $\left(k, p^{e-1}\left(\frac{p^2-1}{2}\right)\right) = 1$, por lo que $k \in \mathbb{Z}^*_{p^{e-1}\left(\frac{p^2-1}{2}\right)}$, y así $\psi(k) = D_k(u)$.

De este modo ψ es un epimorfismo. □

Proposición 3.7. *Sean $p \geq 5$ y ψ el epimorfismo en el corolario 3.6, entonces*

- $Nu(\psi) = \left\{1, -1, p, -p \mod \frac{p^2-1}{2}\right\}$ *si* $e = 1$, *ó*
- $Nu(\psi) = \left\{1, -1 \mod p^{e-1}\left(\frac{p^2-1}{2}\right)\right\}$, *si* $e > 1$.

Demostración. Sea $K = Nu(\psi)$. Si $k \in K$, entonces $D_k(u) = u$ para todo $u \in \mathbb{Z}_{p^e}$.

Aplicamos $D_k(y + y^{-1}) = y^k + y^{-k}$ a toda solución η de (3.1) con $u \in \mathbb{Z}_{p^e}$ arbitrario. Así se tiene $u = \eta + \eta^{-1}$ y

$$D_k(\eta + \eta^{-1}) = \eta^k + \eta^{-k} = \eta + \eta^{-1}.$$

Por lo tanto

$$\eta^k + \eta^{-k} = \eta + \eta^{-1} \tag{3.4}$$

Además usando (3.4) resulta

$$\begin{aligned} 0 &= -1 + 1 = -\eta^k\eta^{-k} + 1 = \eta^k\left[\eta^k - \left(\eta + \eta^{-1}\right)\right] + 1 = \eta^{k+k} - \eta^k\left(\eta + \eta^{-1}\right) + 1 \\ &= \eta^{k+1}\eta^{k-1} - \eta^{k+1} - \eta^{k-1} + 1 = \eta^{k+1}\left[\eta^{k-1} - 1\right] - \left[\eta^{k-1} - 1\right]. \end{aligned}$$

De donde

$$\left(\eta^{k+1} - 1\right)\left(\eta^{k-1} - 1\right) = 0, \tag{3.5}$$

así η es una raíz del polinomio $\left(y^{k+1} - 1\right)\left(y^{k-1} - 1\right) = 0$ y de (3.1), por lo que

$$\left(y^2 - uy + 1\right) \mid \left(y^{k+1} - 1\right)\left(y^{k-1} - 1\right) \quad \text{en } \mathbb{Z}_{p^e}[y]$$

de ahí que existan $s(y), t(y) \in \mathbb{Z}[y]$ tales que

$$\left(y^{k+1} - 1\right)\left(y^{k-1} - 1\right) = s(y)\left(y^2 - uy + 1\right) + p^e t(y) \quad \text{en } \mathbb{Z}[y]. \tag{3.6}$$

Reduciendo módulo p se obtiene

$$\left(y^{k+1} - 1\right)\left(y^{k-1} - 1\right) = s(y)\left(y^2 - uy + 1\right) \ \forall u \in \mathbb{Z}_p \tag{3.7}$$

Sea w un elemento generador del grupo multiplicativo del campo de Galois $\mathbb{F}_{p^2}$. Considerando $v = w^{p-1} + w^{-(p-1)}$ se tiene que $v \in \mathbb{Z}_p$ pues $v^p = v$. Sustituyendo en (3.7) a $v = w^{p-1} + w^{-(p-1)}$ y $y = w^{p-1}$ resulta

$$\left[\left(w^{p-1}\right)^{k+1} - 1\right]\left[\left(w^{p-1}\right)^{k-1} - 1\right] = 0, \tag{3.8}$$

de este modo $\left(w^{p-1}\right)^{k+1} = 1$ ó $\left(w^{p-1}\right)^{k-1} = 1$.

Como $o(w^{p-1}) = p + 1$, entonces

$$(p+1) \mid (k+1) \ \text{ ó } (p+1) \mid (k-1).$$

En [12] se prueba que existe una raíz primitiva módulo p^e, es decir es un generador del grupo $\mathbb{Z}_{p^e}$. Supongamos que g es una de tales raíces y que g^{-1} es su inversa.

Reducimos (3.6) módulo p^e y se obtiene

$$\left(y^{k+1} - 1\right)\left(y^{k-1} - 1\right) = s(y)\left(y^2 - uy + 1\right) \quad \text{en } \mathbb{Z}_{p^e}[y]$$

haciendo $u = g + g^{-1}$ y $y = g$, se tiene

$$\left(g^{k+1} - 1\right)\left(g^{k-1} - 1\right) \equiv 0 \pmod{p^e} \tag{3.9}$$

Si $p|\left(g^{k+1} - 1\right)$ y $p|\left(g^{k-1} - 1\right)$ se tendrá $g^{k+1} \equiv g^{k-1} \pmod{p}$, y por lo tanto $g^2 \equiv 1 \pmod{p}$, pero entonces el orden de g resulta $o(g) = p^{e-1}(p-1) = 2$ de donde $p = 3$, lo que no puede ser pues estamos suponiendo que $p \geq 5$.

Así se deduce de (3.9) que $p^{e-1}(p-1)|(k+1)$ ó $p^{e-1}(p-1)|(k-1)$.

Además, puesto que $(p+1)|(k+1)$ ó $(p+1)|(k-1)$ sólo se cumplen las siguientes cuatro posibilidades para $k \pmod{p^{e-1}\left(\frac{p^2-1}{2}\right)}$:

$$1, -1, k_1 = -1 + (-1)^e p^{e-1}(p-1), k_2 = 1 + (-1)^{e+1} p^{e-1}(p-1).$$

En efecto, pues si $p^{e-1}(p-1)|(k+1)$ y $(p+1)|(k-1)$, entonces

$$\begin{aligned} k &\equiv -1 \pmod{p^{e-1}(p-1)} \text{ y} \\ k &\equiv 1 \pmod{(p+1)} \end{aligned}$$

De la primera congruencia $k = -1 + cp^{e-1}(p-1)$ con $c \in \mathbb{Z}$, sustituyendo en la segunda se obtiene $cp^{e-1}(p-1) \equiv 2 \pmod{(p+1)}$. Pero

$$p^{e-1}(p-1) = (p+1)\left[p^{e-1} - 2p^{e-2} + \cdots + (-1)^{e-1}2\right] + (-1)^e 2$$

y reduciendo módulo $p+1$, resulta que

$$p^{e-1}(p-1) \equiv (-1)^e 2 \pmod{(p+1)}, \tag{3.10}$$

así que $c(-1)^e 2 \equiv 2 \pmod{(p+1)}$. Simplificando se obtiene

$$c(-1)^e \equiv 1 \pmod{\left(\frac{p+1}{2}\right)}$$

de donde

$$c \equiv (-1)^e \pmod{\left(\frac{p+1}{2}\right)}.$$

Por lo tanto

$$\begin{aligned} k &= -1 + \left[(-1)^e + d\left(\frac{p+1}{2}\right)\right] p^{e-1}(p-1) \\ &= -1 + (-1)^e p^{e-1}(p-1) + d\left(\frac{p^{e-1}(p^2-1)}{2}\right). \end{aligned}$$

De ahí que $k \equiv -1 + (-1)^e p^{e-1}(p-1) \pmod{\frac{p^{e-1}\left(p^2-1\right)}{2}}$. Consideremos los siguientes tres posibilidades para los valores de k.

Primer caso.
Si

$$\begin{aligned} k &\equiv 1 \ (\text{mód } p^{e-1}(p-1)) \text{ y} \\ k &\equiv -1 \ (\text{mód } (p+1)) \end{aligned}$$

De la primera congruencia $k = 1 + cp^{e-1}(p-1)$ con $c \in \mathbb{Z}$, sustituyendo en la segunda $cp^{e-1}(p-1) \equiv -2 \ (\text{mód } (p+1))$, y utilizando la ecuación (3.10) se obtiene $c(-1)^e 2 \equiv -2$ (mód $(p+1)$). Simplificando se obtiene

$$c(-1)^e \equiv -1 \ (\text{mód } \left(\frac{p+1}{2}\right))$$

de donde

$$c \equiv (-1)^{e+1} \ (\text{mód } \left(\frac{p+1}{2}\right)).$$

Por lo tanto

$$k = 1 + (-1)^{e+1} p^{e-1} (p-1) + d\left(\frac{p^{e-1}(p^2-1)}{2}\right)$$

De este modo $k \equiv 1 + (-1)^{e+1} p^{e-1} (p-1) \ \left(\text{mód } \frac{p^{e-1}\left(p^2-1\right)}{2}\right)$.

Segundo caso.
Si

$$\begin{aligned} k &\equiv 1 \ (\text{mód } p^{e-1}(p-1)) \text{ y} \\ k &\equiv 1 \ (\text{mód } (p+1)) \end{aligned}$$

De la primera congruencia $k = 1 + cp^{e-1}(p-1)$ con $c \in \mathbb{Z}$, sustituyendo en la segunda $cp^{e-1}(p-1) \equiv 0 \ (\text{mód } (p+1))$, pero por (3.10) se obtiene $c(-1)^e 2 \equiv 0$ (mód $(p+1)$). Simplificando se tiene

$$c(-1)^e \equiv 0 \ (\text{mód } \left(\frac{p+1}{2}\right))$$

de donde

$$c \equiv 0 \ (\text{mód } \left(\frac{p+1}{2}\right))$$

pues $(-1)^e \not\equiv 0 \ (\text{mód } \left(\frac{p+1}{2}\right))$. Así que

$$k = 1 + \left[d\left(\frac{p+1}{2}\right)\right] p^{e-1}(p-1) = 1 + d\left(\frac{p^{e-1}(p^2-1)}{2}\right)$$

Por lo tanto $k \equiv 1 \ \left(\text{mód } \frac{p^{e-1}\left(p^2-1\right)}{2}\right)$.

Tercer caso.
De la misma forma si

$$\begin{aligned} k &\equiv -1 \text{ (mód } p^{e-1}(p-1)) \text{ y} \\ k &\equiv -1 \text{ (mód } (p+1)) \end{aligned}$$

De la primera congruencia $k = -1 + cp^{e-1}(p-1)$ con $c \in \mathbb{Z}$, sustituyendo en la segunda congruencia se tiene $cp^{e-1}(p-1) \equiv 0$ (mód $(p+1)$), pero por (3.10) se obtiene $c(-1)^e 2 \equiv 0$ (mód $(p+1)$). Simplificando nos queda

$$c(-1)^e \equiv 0 \text{ (mód } \left(\frac{p+1}{2}\right))$$

de donde

$$c \equiv 0 \text{ (mód } \left(\frac{p+1}{2}\right))$$

pues $(-1)^e \not\equiv 0$ (mód $\left(\frac{p+1}{2}\right)$). Así que

$$k = -1 + \left[d\left(\frac{p+1}{2}\right)\right] p^{e-1}(p-1) = -1 + d\left(\frac{p^{e-1}(p^2-1)}{2}\right)$$

Por lo tanto $k \equiv -1 \left(\text{mód } \frac{p^{e-1}\left(p^2-1\right)}{2}\right)$

Ahora se distinguen dos subcasos:

- Si $e = 1$ se cumple

$$\begin{aligned} k_1 &= -1 + (-1)(p-1) = -1 - p - 1 = -p \text{ y} \\ k_2 &= 1 + (-1)^2(p-1) = 1 + p - 1 = p \end{aligned}$$

  Sea $v \in \mathbb{Z}_p$ y η una solución de $y^2 - vy + 1 = 0$ en $\mathbb{F}_{p^2}$, entonces $\eta^{p-1} = 1$ ó $\eta^{p+1} = 1$, por lo que en cualquier situación: $\eta^{\frac{p^2-1}{2}} = 1$.

  De este modo $k \equiv \pm 1, \pm p \left(\text{mód } \left(\frac{p^2-1}{2}\right)\right)$. Así siempre $\eta^k + \eta^{-k} = \eta + \eta^{-1}$, por lo que $D_k(\eta + \eta^{-1}) = \eta + \eta^{-1}$ y en consecuencia $K = \{\pm 1, \pm p\}$.

- Cuando $e > 1$, para todo $u \in \mathbb{Z}$ se aplica la fórmula de Taylor

$$D_k(u + p^{e-1}) \equiv D_k(u) + p^{e-1} D_k'(u) \text{ (mód } p^e)$$

  Sea $\bar{k} \in K$ para la clase $\bar{k} \equiv k \left(\text{mód } \frac{p^{e-1}\left(p^2-1\right)}{2}\right)$ a continuación se aplicarán a todas las $u \in \mathbb{Z}$ la relación

$$\begin{aligned} D_k(u) &\equiv u \text{ (mód } p^e) \text{ y} \\ D_k(u + p^{e-1}) &\equiv u + p^{e-1} \text{ (mód } p^e) \end{aligned}$$

Por lo tanto $D'_k(u) \equiv 1 \pmod{p}$, así que para toda $v \in \mathbb{Z}_p$

$$D'_k(v) = 1. \tag{3.11}$$

Por otro lado la derivada está dada por (2.27):

$$D'_k\left(y + \frac{1}{y}\right) = k\left[\frac{y^{2k} - 1}{y^{k-1}(y^2 - 1)}\right].$$

Sea w un elemento generador del grupo multiplicativo de $\mathbb{F}_{p^2}$. Si se hace $y = w^{p-1}$ en (2.27) resulta

$$D'_k\left(w^{p-1} + w^{-(p-1)}\right) = k\left[\frac{w^{2k(p-1)} - 1}{w^{(k-1)(p-1)}(w^2(p-1) - 1)}\right].$$

Nótese que $k_1 \equiv -1 + (-1)^e p^{e-1}(p-1) \left(\text{mód } \frac{p^{e-1}(p^2-1)}{2}\right)$ se obtiene de suponer que $k_1 \equiv 1 \pmod{(p+1)}$, y también $k_2 \equiv 1 + (-1)^{e+1} p^{e-1}(p-1) \left(\text{mód } \frac{p^{e-1}(p^2-1)}{2}\right)$ se consigue de considerar $k_2 \equiv -1 \pmod{(p+1)}$. Y como el orden de w^{p-1} es $o(w^{p-1}) = p + 1$ se sigue que para k_1

$$D'_{k_1}\left(w^{p-1} + w^{-(p-1)}\right) = (-1)\left[\frac{w^{2(p-1)} - 1}{w^2(p-1) - 1}\right] = -1,$$

y para k_2

$$D'_{k_2}\left(w^{p-1} + w^{-(p-1)}\right) = (1)\left[\frac{w^{-2(p-1)} - 1}{w^{-2(p-1)}(w^2(p-1) - 1)}\right] = \frac{w^{-2(p-1)} - 1}{1 - w^{-2(p-1)}} = -1$$

así $\bar{k_1}, \bar{k_2} \notin K$. Pero $1, -1 \in K$ pues

$$D_1\left(y + \frac{1}{y}\right) = y + \frac{1}{y} \text{ y } D_{-1}\left(y + \frac{1}{y}\right) = \frac{1}{y} + y$$

Por lo tanto $K = \{1, -1\}$.

□

3.2. G_{3^e}

Los resultados del caso anterior desde el lema 3.2 hasta el corolario 3.6 se aplican también para $p = 3$. Como en la demostración de la proposición 3.7 se está suponiendo que $Nu(\psi)$ se obtiene para $p \neq 3$, el caso $p = 3$ se estudia por separado.

Lema 3.8. *Sea $e \geq 2$, entonces existen $h_1, h_2 \in \mathbb{Z}$ tales que $h_1 \not\equiv 0$ (mód 3), y polinomios $v_1(y), v_2(y) \in \mathbb{Z}[y]$, de modo que*

$$y^{4\cdot 3^{e-2}} = 1 + 3^{e-1}(h_1 y + h_2) + v_1(y)(y^2 - 3y + 1) + 3^e v_2(y) \tag{3.12}$$

Demostración. Se hará la demostración por inducción sobre e.

Para $e = 2$ aplicamos la congruencia $y^2 \equiv 3y - 1$ (mód $y^2 - 3y + 1$) para calcular y^4 de la siguiente manera:

$$\begin{aligned} y^4 &\equiv (3y-1)^2 \text{ (mód } y^2 - 3y + 1) \\ &\equiv 9(3y-1) - 6y + 1 \text{ (mód } y^2 - 3y + 1) \\ &\equiv 21y - 8 \text{ (mód } y^2 - 3y + 1) \equiv 1 + 3(7y - 3) \text{ (mód } y^2 - 3y + 1) \end{aligned}$$

Por lo tanto (3.12) es válida para $e = 2$.

Supóngase que se satisface la igualdad (3.12) para $e = k$. Entonces existen $\bar{h_1}, \bar{h_2} \in \mathbb{Z}$ tales que $\bar{h_1} \not\equiv 0$ (mód 3), y polinomios $\bar{v_1}(y), \bar{v_2}(y) \in \mathbb{Z}[y]$, de modo que $y^{4\cdot 3^{k-2}} = 1 + 3^{k-1}(\bar{h_1} y + \bar{h_2}) + \bar{v_1}(y)(y^2 - 3y + 1) + 3^k \bar{v_2}(y)$, reduciendo módulo $y^2 - 3y + 1$ se tiene

$$y^{4\cdot 3^{k-2}} \equiv 1 + 3^{k-1}(\bar{h_1} y + \bar{h_2}) + 3^k \bar{v_2}(y) \text{ (mód } y^2 - 3y + 1).$$

Sea $e = k + 1$, elevando al cubo la congruencia anterior resulta:

$$\begin{aligned} y^{4\cdot 3^{k-1}} &= \left(y^{4\cdot 3^{k-2}}\right)^3 = \left(1 + 3^{k-1}(\bar{h_1} y + \bar{h_2}) + 3^k \bar{v_2}(y)\right)^3 \\ &= 1 + 3^k(\bar{h_1} y + \bar{h_2}) + 3^{2k-1}(\bar{h_1} y + \bar{h_2})^2 + 3^{3k-3}(\bar{h_1} y + \bar{h_2})^3 + 3^{k+1}\bar{v_2}(y) \\ &\quad + 3^{2k} 2(\bar{h_1} y + \bar{h_2})\bar{v_2}(y) + 3^{3k-1}(\bar{h_1} y + \bar{h_2})^2 \bar{v_2}(y) + 3^{2k+1}\bar{v_2}^2(y) \\ &\quad + 3^{3k}(\bar{h_1} y + \bar{h_2})\bar{v_2}^2(y) + 3^{3k}\bar{v_2}^3(y) \end{aligned}$$

haciendo $h_1 = \bar{h_1}$, $h_2 = \bar{h_2}$ y factorizando 3^{k+1} del resto de la expresión se obtiene

$$\begin{aligned} y^{4\cdot 3^{k-1}} &= 1 + 3^k(h_1 y + h_2) + 3^{k+1}[3^{k-2}(h_1 y + h_2)^2 + 3^{2k-4}(h_1 y + h_2)^3 \\ &\quad + \bar{v_2}(y) + 3^{k-1} 2(h_1 y + h_2)\bar{v_2}(y) + 3^{2k-2}(h_1 y + h_2)^2 \bar{v_2}(y) \\ &\quad + 3^k \bar{v_2}^2(y) + 3^{2k-1}(h_1 y + h_2)\bar{v_2}^2(y) + 3^{2k-1}\bar{v_2}^3(y)] \end{aligned}$$

de esta manera si v_2 es igual a la expresión entre corchetes en la ecuación anterior, entonces

$$y^{4\cdot 3^{k-1}} = 1 + 3^k(h_1 y + h_2) + 3^{k+1} v_2(y)$$

que es lo que se desea.

□

Teorema 3.9. *Sea $p = 3$, entonces el núcleo de ψ, donde ψ es el epimorfismo del corolario 3.6, es $Nu(\psi) = \{1, -1\}$.*

Demostración. Sea $K = Nu(\psi)$. Como en la demostración de la proposición 3.7 se tiene que $\{1, -1\} \subseteq K$. Se distinguen 3 posibilidades:

- Para $e = 1$, hay que recordar que los valores de k tales que $D_k(x)$ es polinomio de permutación son elegidos de tal manera que $\left(k, p^{e-1}\left(\frac{p^2-1}{2}\right)\right) = 1$, en caso de ser $p = 3$ resulta $p^{e-1}\left(\frac{p^2-1}{2}\right) = 4 \cdot 3^{e-1}$, y para $e = 1$ los posibles valores de k son tales que $(k, 4) = 1$ y estos son $k = 1, -1$.

  Por lo tanto el teorema se cumple en el caso $e = 1$.

- Si $e = 2$, en este caso $p^{e-1}\left(\frac{p^2-1}{2}\right) = 4 \cdot 3^{2-1} = 12$ y así los valores k tales que $(k, 12) = 1$ son $1, -1, 5, -5$, por lo que es suficiente demostrar que $5 \notin K$. Supóngase que $5 \in K$, se utiliza la igualdad (3.11) que es válida para cualquier valor de p, se tiene

  $$D'_5(v) = 1 \text{ para toda } v \in \mathbb{Z}_3.$$

  Tomamos de nuevo a w como un elemento generador del grupo multiplicativo de $\mathbb{F}_{3^2}$, se sustituye w^2 en (2.27) y se obtiene:

  $$D'_5(w^2 + w^{-2}) = (-1)\frac{w^{2\cdot 2\cdot 5} - 1}{w^{2(5-1)}(w^{2(2)} - 1)} = (-1)\frac{w^{20} - 1}{w^8(w^4 - 1)} = (-1)\frac{w^4 - 1}{w^4 - 1} = -1.$$

  Por lo tanto $5 \notin K$, y el teorema es cierto para $e = 2$.

- Para el caso $e > 2$, sea $k \in K$. Si h es una raíz primitiva módulo 3^e, se deduce de la demostración del corolario 3.4 que

  $$\left(h^{k+1} - 1\right)\left(h^{k-1} - 1\right) \equiv 0 \text{ (mód } 3^e) \tag{3.13}$$

  Si $9 | \left(h^{k+1} - 1\right)$ y $9 | \left(h^{k-1} - 1\right)$, entonces $h^2 \equiv 1$ (mód 9) y por tanto h no es una raíz primitiva módulo 9, así que no hay raíz primitiva módulo 3^e, lo que contradice la existencia de h (cf. [12]). Por lo tanto se tiene

  $$2 \cdot 3^{e-2} | (k + 1) \text{ ó } 2 \cdot 3^{e-2} | (k - 1)$$

  así $k = -1 + 2 \cdot 3^{e-2}g$ ó $k = 1 + 2 \cdot 3^{e-2}g$, para algún entero g. Pero como $D_k(u) \equiv u$ (mód 3^e) para todo $u \in \mathbb{Z}$, se sigue que $D_k(u) \equiv u$ (mód 9) para

todo $u \in \mathbb{Z}$, entonces $k \equiv \pm 1$ (mód 12). Pero se consideran a los elementos de K módulo $4 \cdot 3^{e-1}$ y resultan ser:

$$\begin{aligned} k_1 &= 1 + 4 \cdot 3^{e-2} \\ k_2 &= 1 + 8 \cdot 3^{e-2} \\ k_3 &= -1 + 4 \cdot 3^{e-2} \\ k_4 &= -1 + 8 \cdot 3^{e-2} \end{aligned}$$

Además se tiene

$$\begin{aligned} k_2^2 &= 1 + 16 \cdot 3^{e-2} + 64 \cdot 3^{2(e-2)} = 1 + 4 \cdot 3^{e-2} + 4 \cdot 3^{e-1} + 4 \cdot 3^{e-1} \left(16 \cdot 3^{e-3}\right) \\ &= 1 + 4 \cdot 3^{e-2} + 4 \cdot 3^{e-1} \left[1 + 16 \cdot 3^{e-3}\right] = k_1 \\ -k_3 &= -(-1 + 4 \cdot 3^{e-2}) = 1 - 4 \cdot 3^{e-2} + 4 \cdot 3^{e-1} = 1 + 8 \cdot 3^{e-2} = k_2 \\ -k_4 &= -(-1 + 8 \cdot 3^{e-2}) = 1 - 8 \cdot 3^{e-2} + 4 \cdot 3^{e-1} = 1 + 4 \cdot 3^{e-2} = k_1 \end{aligned}$$

Por estas igualdades es suficiente mostrar que $k_1 \notin K$, y supóngase que $k_1 \in K$ para lo que se considera η, la clase de residuos en el anillo $\mathbb{Z}_3[y]/\langle y^2 - 3y + 1\rangle$. Entonces por (3.5) con k_1 en lugar de k se tiene:

$$\left(\eta^{4 \cdot 3^{e-2}} - 1\right)\left(\eta^{4 \cdot 3^{e-2}+2} - 1\right) = 0. \tag{3.14}$$

Debido a la ecuación (3.12) se cumple que

$$\eta^{4 \cdot 3^{e-2}} = 1 + 3^{e-1}(h_1\eta + h_2). \tag{3.15}$$

Empleamos esta expresión en (3.14) y se obtiene

$$3^{e-1}(h_1\eta + h_2)\left[\left(1 + 3^{e-1}(h_1\eta + h_2)\right)\eta^2 - 1\right] = 0.$$

Como $\eta^2 - 3\eta + 1 = 0$, entonces $\eta^2 = 3\eta - 1$ así

$$3^{e-1}(h_1\eta + h_2)\left[\left(1 + 3^{e-1}(h_1\eta + h_2)\right)(3\eta - 1) - 1\right] = 0$$

y por lo tanto si

$$\left(1 + 3^{e-1}(h_1\eta + h_2)\right)(3\eta - 1) = 1$$

entonces $3\eta\left(1 + 3^{e-1}(h_1\eta + h_2)\right) - 1 - 3^{e-1}(h_1\eta + h_2) = 1$, y de aquí

$$3\eta + 3^e\eta(h_1\eta + h_2) - 3^{e-1}(h_1\eta + h_2) = 2$$

de este modo $2 \cdot 3^{e-1}(h_1\eta + h_2) = 0$. Por lo tanto en $\mathbb{Z}[y]$ es una ecuación de la forma

$$2 \cdot 3^{e-1}(h_1\eta + h_2) = u_1(y)(y^2 - 3y + 1) + 3^e u_2(y)$$

con $u_1(y) = 3^{e-1}w(y)$, donde $w(y) \in \mathbb{Z}[y]$ y dividiendo entre 3^{e-1} se obtiene

$$2(h_1\eta + h_2) = w(y)(y^2 - 3y + 1) + 3u_2(y).$$

así $w(y) = 3w_1(y)$, una contradicción de que $h_1 \not\equiv 0$ (mód 3), según el lema 3.8. De esta forma $K = \{1, -1\}$.

□

3.3. G_{2^e}

Lema 3.10. *Sean $e \geq 4$ y $u \equiv 1$ (mód 2), entonces existen $h_1, h_2 \in \mathbb{Z}$ y $v_1(y), v_2(y) \in \mathbb{Z}[y]$ tales que*

$$y^{3\cdot 2^{e-3}} = 1 + 2^{e-1}(h_1 y + h_2) + v_1(y)(y^2 - uy + 1) + 2^e v_2(y). \tag{3.16}$$

Demostración. Se procede por inducción sobre e.

Como $y^2 \equiv uy - 1$ (mód $y^2 - uy + 1$), se sigue que:

$$y^3 \equiv (uy-1)y \text{ (mód } y^2 - uy + 1) \equiv u(uy-1) - y \text{ (mód } y^2 - uy + 1).$$

Por lo tanto $y^3 \equiv (u^2-1)y - u$ (mód $y^2 - uy + 1$), el cual elevamos al cuadrado para tener:

$$\begin{aligned} y^6 &\equiv (u^2-1)^2y^2 - 2u(u^2-1)y + u^2 \text{ (mód } y^2 - uy + 1) \\ &\equiv (u^2-1)^2uy - (u^2-1)^2 - 2u(u^2-1)y + u^2 \text{ (mód } y^2 - uy + 1) \\ &\equiv \left[u(u^2-1)^2 - 2u(u^2-1)\right] y + u^2 - (u^2-1)^2 \text{ (mód } y^2 - uy + 1) \end{aligned}$$

así que

$$y^6 \equiv u(u^2-1)(u^2-3)y + u^2 - (u^2-1)^2 \text{ (mód } y^2 - uy + 1). \tag{3.17}$$

Como $u \equiv 1$ (mód 2), entonces $u = 2t+1$, y así $u^2-1 = 4(t^2+t)$ y $u^2-3 = 2(2t^2+2t-1)$. Por lo tanto

$$u(u^2-1)(u^2-3) = 8(2t+1)(t^2+t)(2t^2+2t-1)$$

y se sigue que $u(u^2-1)(u^2-3) \equiv 0$ (mód 8).

Nótese que $t^2 + t = 2s$ con $s \in \mathbb{Z}$, por lo que $u^2 = 8s + 1$. De este modo

$$u^2 - (u^2-1)^2 = 1 + 8s - 16(t^2+t)^2 = 1 + 8\left(s + 2(t^2+t)^2\right)$$

de ahí que $u^2 - (u^2-1)^2 \equiv 1$ (mód 8) y el lema se cumple para $e = 3$.

Ahora supóngase que el lema se satisface para $e = k$, es decir suponemos que existen $\bar{h_1}, \bar{h_2} \in \mathbb{Z}$ y $\bar{v_1}(y), \bar{v_2}(y) \in \mathbb{Z}[y]$ tales que

$$y^{3\cdot 2^{k-3}} = 1 + 2^{k-1}(\bar{h_1} y + \bar{h_2}) + \bar{v_1}(y)(y^2 - uy + 1) + 2^k \bar{v_2}(y).$$

Sea $e = k+1$, elevando a la cuarta potencia la igualdad del caso $e = 3$, y sustituyendo $h_1 = \bar{h_1}$, $h_2 = \bar{h_2}$,

$$v_1(y) = \bar{v_1}(y)\left[\bar{v_1}(y)(y^2 - uy + 1) + 2^k(\bar{h_1} y + \bar{h_2}) + 2\right] \text{ y}$$

$$v_2(y) = 2^{k-3}(\bar{h_1} y + \bar{h_2})^2 + 2^{k-1}\bar{v_2}(y)\left((\bar{v_2}(y)) + \bar{h_1} y + \bar{h_2}\right) + \bar{v_2}(y) + \bar{v_1}(y)\bar{v_2}(y)(y^2 - uy + 1)$$

se obtiene el resultado deseado, que es:

$$y^{3\cdot 2^{k-2}} = 1 + 2^k(h_1 y + h_2) + v_1(y)(y^2 - uy + 1) + 2^{k+1} v_2(y).$$

□

Corolario 3.11. *Sea $e \geq 4$, entonces existen $h_1, h_2 \in \mathbb{Z}$ con $h_1 \equiv 0$ (mód 2), $h_2 \equiv 1$ (mód 2) y $v_1(y), v_2(y) \in \mathbb{Z}[y]$ tales que*

$$y^{3\cdot 2^{e-3}} = 1 + 2^{e-1}(h_1 y + h_2) + v_1(y)(y^2 - 3y + 1) + 2^e v_2(y). \tag{3.18}$$

Demostración. Como antes el corolario se prueba por inducción sobre e.

La ecuación que se considera en el lema 3.10 es $y^2 - uy + 1 = 0$, en este caso $u = 3$ y de (3.16) se tiene que $y^6 \equiv 3 \cdot 8 \cdot 6y + 1 + 8 - 8 \cdot 8$ (mód $y^2 - 3y + 1$). Reduciendo nos queda $y^6 \equiv 8(18y - 7) + 1$ (mód $y^2 - 3y + 1$) con lo que se cumple (3.18) para $e = 4$ pues $h_1 = 18 \equiv 0$ (mód 2) y $h_1 = -7 \equiv 1$ (mód 2).

Supóngase ahora que para $e = k$ existen $\bar{h_1}, \bar{h_2} \in \mathbb{Z}$ con $\bar{h_1} \equiv 0$ (mód 2), $\bar{h_2} \equiv 1$ (mód 2) y $\bar{v_1}(y), \bar{v_2}(y) \in \mathbb{Z}[y]$ tales que

$$y^{3\cdot 2^{k-3}} = 1 + 2^{k-1}(\bar{h_1} y + \bar{h_2}) + \bar{v_1}(y)(y^2 - 3y + 1) + 2^k \bar{v_2}(y).$$

Para probar que se cumple (3.18) siendo $e = k + 1$ notemos que de la demostración del lema 3.10, con $h_1 = \bar{h_1}$, $h_2 = \bar{h_2}$, se tienen las igualdades

$$v_1(y) = \bar{v_1}(y)\left[\bar{v_1}(y)(y^2 - uy + 1) + 2^k(\bar{h_1} y + \bar{h_2}) + 2\right] \text{ y}$$

$$v_2(y) = 2^{k-3}(\bar{h_1} y + \bar{h_2})^2 + 2^{k-1}\bar{v_2}(y)\left((\bar{v_2}(y)) + \bar{h_1} y + \bar{h_2}\right) + \bar{v_2}(y) + \bar{v_1}(y)\bar{v_2}(y)(y^2 - uy + 1)$$

de donde $h_1 \equiv 0$ (mód 2) y $h_2 \equiv 1$ (mód 2), con lo que se demuestra que (3.18) se cumple para $e = k + 1$. □

En seguida se prueban resultados análogos al lema 3.10, que en conjunto nos ayudarán a alcanzar el objetivo del caso 3.

Lema 3.12. *Sean $e \geq 3$ y $u \equiv 0$ (mód 4), entonces existen $v_1(y), v_2(y) \in \mathbb{Z}[y]$ tales que:*

$$y^{2^{e-1}} = 1 + v_1(y)(y^2 - uy + 1) + 2^e v_2(y) \tag{3.19}$$

Demostración. La demostración se hará por inducción sobre e.

Se tiene que $y^2 \equiv uy - 1$ (mód $y^2 - uy + 1$) el cual elevamos al cuadrado para calcular y^4, como $(uy - 1)^2 = u^2y^2 - 2uy + 1$, se sustituye de nuevo el valor de y^2 y se obtiene:

$$y^4 \equiv u^2(uy - 1) - 2uy + 1 \text{ (mód } y^2 - uy + 1) \equiv u^3 y - u^2 - 2uy + 1 \text{ (mód } y^2 - uy + 1)$$

simplificando resulta $y^4 \equiv u(u^2 - 2)y + 1 - u^2$ (mód $y^2 - uy + 1$), por lo que existe $v_1(y) \in \mathbb{Z}[y]$ tal que $y^4 \equiv u(u^2 - 2)y + 1 - u^2 + v_1(y)(y^2 - uy + 1)$.

Como $u \equiv 0$ (mód 4), entonces $u = 2^2 t$ con $t \in \mathbb{Z}$, al sustituir el valor de u en la igualdad anterior queda:

$$\begin{aligned} y^4 &= 1 + 2^2 t(2^4 t^2 - 2)y - 2^4 t^2 + v_1(y)(y^2 - uy + 1) \\ &= 1 + 2^3\left[t\left(2^3 t^2 - 1\right)y - 2t^2\right] + v_1(y)(y^2 - uy + 1). \end{aligned}$$

Sea $v_2(y) = t\left(2^3t^2 - 1\right)y - 2t^2$, de esta manera $y^4 = 1 + v_1(y)(y^2 - uy + 1) + 2^3v_2(y)$, por lo que (3.19) se cumple cuando $e = 3$.

Para $e = k$, supóngase la existencia de $\bar{v_1}(y), \bar{v_2}(y) \in \mathbb{Z}[y]$ con la siguiente propiedad:

$$y^{2^{k-1}} = 1 + \bar{v_1}(y)(y^2 - uy + 1) + 2^k\bar{v_2}(y).$$

Sea ahora $e = k + 1$, y se tiene que $y^{2^k} = \left(y^{2^{k-1}}\right)^2$, por lo que

$$\begin{aligned} y^{2^k} &= \left[1 + \bar{v_1}(y)(y^2 - uy + 1) + 2^e\bar{v_2}(y)\right]^2 \\ &= 1 + \left[2\bar{v_1}(y) + \bar{v_1}^2(y) + 2^{e+1}\bar{v_1}(y)\bar{v_2}(y)\right](y^2 - uy + 1) + 2^{e+1}\left[\bar{v_2}(y) + \bar{v_2}^2(y)\right] \end{aligned}$$

Considerando $v_1(y) = 2\bar{v_1}(y) + \bar{v_1}^2(y) + 2^{e+1}\bar{v_1}(y)\bar{v_2}(y)$ y $v_2(y) = \bar{v_2}(y) + \bar{v_2}^2(y)$, se tiene el resultado deseado.

□

El siguiente resultado es análogo al del lema 3.12, pero difieren en cómo se considera el valor de u.

Lema 3.13. *Sea $e \geq 2$ y $u \equiv 2$ (mód 4), entonces existen $v_1(y), v_2(y), v_3(y) \in \mathbb{Z}[y]$ tales que :*

$$y^{2^{e-1}} = 1 + v_1(y)(y^2 - uy + 1) + 2^{e-1}(y - 1)v_2(y) + 2^e v_3(y) \tag{3.20}$$

Demostración. La demostración se hará por inducción sobre e.

Como $y^2 \equiv uy - 1$ (mód $y^2 - uy + 1$) y $u \equiv 2$ (mód 4), entonces $u = 4g + 2$ con $g \in \mathbb{Z}$, de donde se sigue que

$$y^2 \equiv 4gy + 2y - 1 \text{ (mód } y^2 - uy + 1) \equiv 1 + 2(y - 1) + 4gy \text{ (mód } y^2 - uy + 1).$$

Considerando $v_2(y) = 1$ y $v_3(y) = gy$ se tiene que

$$y^2 = 1 + v_1(y)(y^2 - uy + 1) + 2(y - 1)v_2(y) + 2^2 v_3(y) \tag{3.21}$$

por lo que se cumple (3.20) para $e = 2$.

Supóngase que se cumple para $e = k$, es decir que existen $\bar{v_1}(y), \bar{v_2}(y), \bar{v_3}(y) \in \mathbb{Z}[y]$ tales que $y^{2^{k-1}} = 1 + \bar{v_1}(y)(y^2 - uy + 1) + 2^{k-1}(y - 1)\bar{v_2}(y) + 2^k\bar{v_3}(y)$.

Sea $e = k + 1$, nótese que y^{2^k} se obtiene de elevar al cuadrado $y^{2^{k-1}}$ de tal manera que se tiene

$$y^{2^k} = \left[1 + \bar{v_1}(y)(y^2 - uy + 1) + 2^{e-1}(y - 1)\bar{v_2}(y) + 2^e\bar{v_3}(y)\right]^2.$$

Desarrollando el cuadrado, factorizando y considerando

$$v_1(y) = 2\bar{v_1}(y) + 2^k\bar{v_1}(y)(y - 1)\bar{v_2}(y) + 2^{k+1}\bar{v_1}(y)\bar{v_3}(y) + \bar{v_1}^2(y)(y^2 - uy + 1)$$

$$v_2(y) = (y - 1)\bar{v_2}^2(y) + \bar{v_2}(y) + 2^k\bar{v_2}(y)\bar{v_3}(y) \text{ y } v_3(y) = \bar{v_3}(y) + \bar{v_3}^2(y)$$

se obtiene la siguiente igualdad

$$y^{2^k} = 1 + v_1(y)(y^2 - uy + 1) + 2^k(y-1)v_2(y) + 2^{k+1}v_3(y),$$

con lo que se cumple (3.20).

□

Corolario 3.14. *Sean $e \geq 3$ y $v \in \mathbb{Z}_{2^e}$. Si $v \equiv 1$ (mód 2), entonces la ecuación $y^2 - vy + 1 = 0$ tiene una solución η en una extensión del anillo $\mathbb{Z}_{2^e}$ con $\eta^{3\cdot 2^{e-2}} = 1$. Y si $v \equiv 0$ (mód 2), la ecuación $y^2 - vy + 1 = 0$ tiene una solución η en una extensión del anillo $\mathbb{Z}_{2^e}$ con $\eta^{2^{e-1}} = 1$.*

Demostración. Se considera primero el caso en el que $v \equiv 1$ (mód 2), entonces por (3.16) y satisface

$$y^{3\cdot 2^{e-2}} = 1 + 2^e(h_1 y + h_2) + v_1(y)(y^2 - vy + 1) + 2^{e+1}v_2(y)$$

de esta manera la clase de residuos η de y en $\mathbb{Z}_{2^e}[y]/\langle y^2 - vy + 1\rangle$ cumple

$$\eta^{3\cdot 2^{e-2}} = 1 \in \mathbb{Z}_{2^e}[y]/\left\langle y^2 - vy + 1\right\rangle$$

Ahora si $v \equiv 0$ (mód 2), se tienen 2 casos: $v \equiv 0$ (mód 4) ó $v \equiv 2$ (mód 4), en el primer caso por (3.17) se tiene que la clase de residuos η de y en $\mathbb{Z}_{2^e}[y]/\langle y^2 - vy + 1\rangle$ satisface $\eta^{2^{e-1}} = 1$. Y si $v \equiv 2$ (mód 4), de manera similar a la demostración del lema 3.2 se tiene que $\mathbb{Z}_{2^e}[y]/\langle (y-1)^2 - 2^{e-2}gy, 2^{e-2}(y-1)\rangle$ es una extensión de $\mathbb{Z}_{2^e}$, así que la clase de residuos η de y cumple $(\eta-1)^2 - 2^{e-2}g\eta = 0$ y $2^{e-2}(\eta-1)$, de esta manera:

$$\begin{aligned}\eta^{2^{e-1}} &= [(\eta-1)+1]^{2^{e-1}} = \left[\sum_{i=0}^{2^{e-2}} \binom{2^{e-2}}{i}(\eta-1)^i\right]^2 = \left[(\eta-1)^{2^{e-2}} + 1\right]^2 \\ &= \left[(\eta-1)^2(\eta-1)^{2^{e-3}} + 1\right]^2 = \left[2^{e-2}(\eta-1)g\eta(\eta-1)^{2^{e-4}} + 1\right]^2 = 1.\end{aligned}$$

Por lo tanto $\eta^{2^{e-1}} = 1$, como se deseaba probar.

□

Proposición 3.15. *Sean $k, l > 0$ y $k \equiv l$ (mód $3 \cdot 2^{e-1}$), entonces*

$$D_k(u) \equiv D_l(u) \text{ (mód } 2^e) \text{ para todo } u \in \mathbb{Z}$$

Demostración. Sean $u \in \mathbb{Z}$ y $v = u$ mód 2^e. Como $k \equiv l$ (mód $3 \cdot 2^{e-1}$), entonces $k = l + 3 \cdot 2^{e-1}t$ con $t \in \mathbb{Z}$.

Para $e \geq 3$ por el corolario 3.14 existe η en una extensión de $\mathbb{Z}_{2^e}$ tal que η es solución de $y^2 - vy + 1 = 0$, y como ya se ha visto se tiene que $v = \eta + \eta^{-1}$.

Si $v \equiv 1 \pmod 2$ se cumple que $\eta^{3\cdot 2^{e-2}} = 1$, así en $\mathbb{Z}_{2^e}$ son válidas las siguientes igualdades

$$\begin{aligned} D_k(v) &= D_k(\eta+\eta^{-1}) = \eta^k + \eta^{-k} = \eta^{l+3\cdot 2^{e-1}t} + \eta^{-l-3\cdot 2^{e-1}t} \\ &= \eta^l \left(\eta^{3\cdot 2^{e-2}}\right)^{2t} + \eta^{-l}\left(\eta^{3\cdot 2^{e-2}}\right)^{-2t} = \eta^l + \eta^{-l} = D_l(v). \end{aligned}$$

Si $v \equiv 0 \pmod 2$, entonces $\eta^{2^{e-1}} = 1$ por lo que en $\mathbb{Z}_{2^e}$ se satisface

$$\begin{aligned} D_k(v) &= D_k(\eta+\eta^{-1}) = \eta^k + \eta^{-k} = \eta^{l+3\cdot 2^{e-1}t} + \eta^{-l-3\cdot 2^{e-1}t} \\ &= \eta^l \left(\eta^{2^{e-1}}\right)^{3t} + \eta^{-l}\left(\eta^{2^{e-1}}\right)^{-3t} = \eta^l + \eta^{-l} = D_l(v). \end{aligned}$$

Ahora para el caso $e = 1$, se tiene que $k \equiv l \pmod 3$ por lo que $k = l + 3t$ con $t \in \mathbb{Z}$ y además una solución η de $y^2 - vy + 1 = 0$ en $GF(4)$ siempre cumple que $\eta^3 = 1$, así en $\mathbb{Z}_{2^e}$:

$$D_k(v) = D_k(\eta+\eta^{-1}) = \eta^k+\eta^{-k} = \eta^{l+3t}+\eta^{-l-3t} = \eta^l\left(\eta^3\right)^t+\eta^{-l}\left(\eta^3\right)^{-t} = \eta^l+\eta^{-l} = D_l(v)$$

En el caso $e = 2$, de (3.17) y (3.21) se cumplen las siguientes congruencias:

$$\begin{aligned} y^6 &\equiv v(v^2-1)(v^2-3)y + v^2 - (v^2-1)^2 \pmod{y^2 - vy + 1} \\ y^2 &\equiv 1 + 2(y-1) + 2^2 gy \pmod{y^2 - vy + 1} \end{aligned}$$

de donde la ecuación $y^2 - vy + 1 = 0$ tiene una solución η en la extensión de $\mathbb{Z}_4$ que es $\mathbb{Z}_4[y]/\langle y^2 - vy + 1, y\rangle$, así se tienen $\eta^6 = v(v^2-1)(v^2-3)\eta + v^2 - (v^2-1)^2$ y $\eta^2 = 1 + 2(\eta - 1) = -1 + 2\eta$.

De $\eta^2 = -1 + 2\eta$, se obtiene $\eta^2 = -1$. Y de $\eta^6 = v(v^2-1)(v^2-3)\eta + v^2 - (v^2-1)^2$ se tienen las opciones respecto al valor de v:

1. Si $v \equiv 0 \pmod 4$, $\eta^6 = 1$.
2. En el caso $v \equiv 1 \pmod 4$, $\eta^6 = 1$.
3. Ahora si $v \equiv 2 \pmod 4$, $\eta^6 = 2(2^2-1)(2^2-3)\eta + 2^2 - (2^2-1)^2 = 2\eta - 1$, dado que η es solución de $y^2 - vy + 1 = 0$ se tiene $\eta^2 = -1 + 2\eta$, así que como ya se demostró $\eta^2 = -1$.
4. Si $v \equiv 3 \pmod 4$, entonces $\eta^6 = 3(3^2-1)(3^2-3)\eta + 3^2 - (3^2-1)^2 = 1$.

Por lo tanto $\eta^6 = 1$ ó $\eta^2 = -1$, así $\eta^{12} = 1$ en cualquier caso. Además $k = l + 6t$ por lo que

$$\begin{aligned} D_k(v) - D_l(v) &= \eta^k + \eta^{-k} - \eta^l - \eta^{-l} = \eta^{l+6t} + \frac{1}{\eta^{l+6t}} - \eta^l - \frac{1}{\eta^l} \\ &= \frac{\eta^{2l} + 1 - \eta^{2l+6t} - \eta^{6t}}{\eta^{l+6t}} = \frac{\left(\eta^{2l}+1\right)\left(1-\eta^{6t}\right)}{\eta^{l+6t}} \end{aligned}$$

para que $D_l(x)$ sea polinomio de permutación mód 4, l tiene que ser impar, de donde $\eta^{2l} = \eta^2$, y como $\eta^6 = 1$ ó $\eta^2 = -1$, entonces

$$D_k(v) - D_l(v) = \frac{(\eta^2+1)(1-\eta^{6t})}{\eta^{l+6t}} = 0$$

De esta manera en $\mathbb{Z}_4$ se tiene $D_k(v) = D_l(v)$. □

Lema 3.16. *Sea $e \geq 3$, entonces*

$$D_{3\cdot 2^{e-2}+1}(u) \equiv u \ (\textit{mód } 2^e) \textit{ para todo } u \in \mathbb{Z}$$

Demostración. Sean $k = 3\cdot 2^{e-2}+1$, $v = u$ mód 2^e y considérese la ecuación $y^2 - vy + 1 = 0$. Se analizan por separado las opciones v impar y v par:

1. Si $v \equiv 1$ (mód 2), por el corolario 3.14 la ecuación $y^2 - vy + 1 = 0$ tiene una solución η en una extensión de $\mathbb{Z}_{2^e}$ tal que $\eta^{3\cdot 2^{e-2}} = 1$ y $v = \eta + \eta^{-1}$, así $\eta^k = \eta^{3\cdot 2^{e-2}+1} = \eta^{3\cdot 2^{e-2}}\eta = \eta$, por lo que $D_k(v) = \eta^k + \eta^{-k} = \eta + \eta^{-1} = v$, que es el resultado deseado.

2. Si $v \equiv 0$ (mód 2), por el corolario 3.14 la ecuación $y^2 - vy + 1 = 0$ tiene una solución η en una extensión de $\mathbb{Z}_{2^e}$ tal que $\eta^{2^{e-1}} = 1$, de este modo

$$\begin{aligned} D_k(v) - v &= \eta^k + \frac{1}{\eta^k} - \eta - \frac{1}{\eta} = \frac{\eta^{2k} + 1 - \eta^{k+1} - \eta^{k-1}}{\eta^k} \\ &= \frac{\eta^{3\cdot 2^{e-1}+2} + 1 - \eta^{3\cdot 2^{e-2}+2} - \eta^{3\cdot 2^{e-2}}}{\eta^k} = \frac{\eta^2 + 1 - \eta^{3\cdot 2^{e-2}}\eta^2 - \eta^{3\cdot 2^{e-2}}}{\eta^k}. \end{aligned}$$

Así $D_k(v) - v = \frac{(\eta^2+1)\left(1-\eta^{3\cdot 2^{e-2}}\right)}{\eta^k}$. Además $3 \cdot 2^{e-2} = 2^{e-1} + 2^{e-2}$ por lo que $\eta^{3\cdot 2^{e-2}} = \eta^{2^{e-1}}\eta 2^{e-2} = \eta^{2^{e-2}}$ de esta manera se tiene:

$$D_k(v) - v = \frac{(\eta^2+1)\left(1-\eta^{2^{e-2}}\right)}{\eta^k}. \tag{3.22}$$

Debido a que η es solución de $y^2 - vy + 1 = 0$, se tiene $\eta^2 + 1 = v\eta$. Notemos que si $v \equiv 0$ (mód 4), entonces $v = 4t_1$ con $t_1 \in \mathbb{Z}$, y si $v \equiv 2$ (mód 4), $v = 2(2t_2+1)$ con $t_2 \in \mathbb{Z}$. Así que para el primer factor se tiene:

$$\eta^2 + 1 = \begin{cases} 4s_1, & \text{si } v \equiv 0 \text{ (mód 4)} \\ 2s_2, & \text{si } v \equiv 2 \text{ (mód 4)} \end{cases}$$

Si $e = 3$, por (3.19), en $\mathbb{Z}_{2^3}$ se satisface $1 - \eta^2 = 1 - (v\eta - 1) = 2 - v\eta$, por lo que si $v \equiv 0$ (mód 4), entonces $1 - \eta^2 = 2 - 4t_1\eta = 2(1 - 2t_1\eta)$. Y para $e > 3$ de nuevo por (3.19) se tiene que $1 - \eta^{2^{e-2}} = 2^{e-1}v_2(\eta)$, en consecuencia si $v \equiv 0$ (mód 4) resulta

$$1 - \eta^{2^{e-2}} = \begin{cases} 2m_1, & \text{si } e = 3 \\ 2^{e-1}m_2, & \text{si } e > 3 \end{cases}$$

En el caso $v \equiv 2$ (mód 4) por (3.20) se tiene $1 - \eta^{2^{e-2}} = 2^{e-1}v_3(\eta)$.

Así, cuando $v \equiv 0$ (mód 4) se cumple que

$$(\eta^2 + 1)(1 - \eta^{2^{e-2}}) = \begin{cases} 8s_1m_1, & \text{si } e = 3 \\ 4 \cdot 2^{e-1}s_2m_2, & \text{si } e > 3 \end{cases}$$

de donde $(\eta^2 + 1)(1 - \eta^{2^{e-2}}) \equiv 0$ (mód 2^e) para $e \geq 3$.

Y si $v \equiv 2$ (mód 4), se tiene $(\eta^2 + 1)(1 - \eta^{2^{e-2}}) = 2^e s_2 v_3(\eta)$ para $e \geq 3$, y se sigue que $(\eta^2 + 1)(1 - \eta^{2^{e-2}}) \equiv 0$ (mód 2^e). Por lo tanto $D_k(v) - v \equiv 0$ (mód 2^e).

□

Proposición 3.17. *Sean $e \geq 3$, $k, l \in \mathbb{N}$ impares y $k \equiv l$ (mód $3 \cdot 2^{e-2}$), entonces*

$$D_k(u) \equiv D_l(u) \text{ (mód } 2^e) \text{ para todo } u \in \mathbb{Z}$$

Demostración. Como $k \equiv l$ (mód $3 \cdot 2^{e-2}$), entonces $k = l + 3 \cdot 2^{e-2}g$ con $g \in \mathbb{Z}$. Así

$$k \equiv l \text{ (mód } 3 \cdot 2^{e-1}) \text{ ó } k \equiv l + 3 \cdot 2^{e-2} \text{ (mód } 3 \cdot 2^{e-1}).$$

En el caso de que $k \equiv l$ (mód $3 \cdot 2^{e-1}$) por la proposición 3.15 se obtiene el resultado deseado.

Y si $k \equiv l + 3 \cdot 2^{e-2}$ (mód $3 \cdot 2^{e-1}$), como $l = 2t + 1$ para un $t \in \mathbb{Z}$, se cumple:

$$\begin{aligned} k &\equiv l + 3 \cdot 2^{e-2} + 3 \cdot 2^{e-1}t \text{ (mód } 3 \cdot 2^{e-1}) \equiv l + (2t+1)3 \cdot 2^{e-2} \text{ (mód } 3 \cdot 2^{e-1}) \\ &\equiv l + l3 \cdot 2^{e-2} \text{ (mód } 3 \cdot 2^{e-1}) \equiv l(1 + 3 \cdot 2^{e-2}) \text{ (mód } 3 \cdot 2^{e-1}) \end{aligned}$$

Utilizando la proposición 3.15 y el lema 3.16 se tiene para $v = u \mod 2^e$:

$$D_k(v) = D_{l(1+3\cdot 2^{e-2})}(v) = D_l\left(D_{1+3\cdot 2^{e-2}}(v)\right) \equiv D_l(u) \text{ (mód } 2^e)$$

Por lo tanto $D_k(u) \equiv D_l(u)$ (mód 2^e).

□

Teorema 3.18. *Para cada $a \in \mathbb{Z}_{2^e}$ y si $e < 3$, entonces la función ψ definida como:*

$$\psi : \mathbb{Z}^*_{2^{e-1}\cdot 3} \to G_{2^e}$$

$$\psi(k) = D_k(a)$$

es un epimorfismo.

Si $e \geq 3$, entonces la función ψ definida para cada $a \in \mathbb{Z}_{2^e}$ como:

$$\psi : \mathbb{Z}^*_{2^{e-2}\cdot 3} \to G_{2^e}$$

$$\psi(k) = D_k(a)$$

es un epimorfismo.

Demostración. La demostración es idéntica a la del corolario 3.6. □

Teorema 3.19. *Para el núcleo del epimorfismo ψ del teorema 3.18 se tiene siempre que* $Nu(\psi) = \{ \overline{1}, \overline{-1} \}$

Demostración. Sea $K_e = Nu(\psi)$. Como $\overline{1} \in K_e$, falta por demostrar que $\overline{-1} \in K_e$.

Para $e \geq 3$. Sea $v = \eta + \frac{1}{\eta}$, η y v como en el corolario 3.14 del que se tiene

$$\eta^{2^{e-2}\cdot 3} = 1 \text{ o } \eta^{2^{e-1}} = 1$$

de donde

$$\eta^{2^{e-1}\cdot 3-1} = \begin{cases} \eta^{2^{e-2}\cdot 2\cdot 3-1} = \eta^{-1} \\ \eta^{2^{e-1}\cdot 3-1} = \eta^{-1} \end{cases}$$

además $\eta^{-2^{e-1}\cdot 3+1} = \eta$.

Por lo que si $k = 2^{e-1} \cdot 3 - 1$, se satisface en $\mathbb{Z}_{2^e}$

$$D_k(v) = \eta^k + \frac{1}{\eta^k} = \frac{1}{\eta} + \eta = v$$

así $k = 2^{e-1} \cdot 3 - 1 \in K_e$.

Para $e < 3$, $5 = \overline{-1} \in \mathbb{Z}_{2^{e-2}\cdot 3}$, por lo que $D_5(v) = v$. De esta manera $\{ \overline{1}, \overline{-1} \} \subseteq K_e$.

Ahora sea $e < 3$ y $k \in \mathbb{Z}^*_{2^{e-1}\cdot 3}$, de donde se tienen los siguientes casos:

- Si $e = 2$, $k \in \mathbb{Z}^*_6 = \{1, 5\} = \{ \overline{1}, \overline{-1} \}$.
- Si $e = 2$, $k \in \mathbb{Z}^*_3 = \{1, 2\} = \{ \overline{1}, \overline{-1} \}$.

de aquí se ve que el orden de $\mathbb{Z}_6^*$ y $\mathbb{Z}_3^*$ es 2, por lo que para $e < 3$ se cumple $K_e = \{\ \overline{1}, \overline{-1}\ \}$.

Si $e \geq 3$ y $k \in \mathbb{Z}^*_{2^{e-2}\cdot 3}$. La proposición 3.17 muestra que si $k \in K_{e+1}$, entonces $D_k(a) \equiv a \pmod{2^e}$. Por lo tanto $k \equiv \pm 1 \pmod{2^{e-2}\cdot 3}$ de modo que $k \equiv \pm 1 \pmod{2^{e-1}\cdot 3}$ o $k \equiv \pm 1 + 2^{e-2}\cdot 3 \pmod{2^{e-1}\cdot 3}$. Además

$$\begin{aligned} -1 + 2^{e-2}\cdot 3 &\equiv -1 + 2^{e-2}\cdot 3 - 2^{e-1}\cdot 3 \pmod{2^{e-1}\cdot 3} \\ &\equiv -1 - 2^{e-2}\cdot 3(-1+2) \pmod{2^{e-1}\cdot 3} \equiv -(1 + 2^{e-2}\cdot 3) \pmod{2^{e-1}\cdot 3} \end{aligned}$$

De la igualdad anterior basta con mostrar que $k = 1 + 2^{e-2}\cdot 3 \notin K_{e+1}$, o en otras palabras para $k = 1 + 2^{e-3}\cdot 3$ y $e \geq 4$, $k \notin K_e$.

Supóngase que $k \in K_e$, al igual que η para cada solución de $y^2 - 3y + 1 = 0$ que se encuentra en una extensión del anillo $\mathbb{Z}_{2^e}$ se aplica que $\eta^k + \frac{1}{\eta^k} = \eta + \frac{1}{\eta}$, es decir

$$\left(\eta^{k-1} - 1\right)\left(\eta^{k+1} - 1\right) = 0,$$

pero $k = 1 + 2^{e-3}\cdot 3$ de donde $k + 1 = 2 + 2^{e-3}\cdot 3$ y $k - 1 = 2^{e-3}\cdot 3$ por lo que

$$\left(\eta^{2^{e-3}\cdot 3} - 1\right)\left(\eta^{2+2^{e-3}\cdot 3} - 1\right) = 0. \tag{3.23}$$

Además η es la raíz en la clase de residuos de y en $\mathbb{Z}_{2^e}[y] \,/\, \langle y^2 - 3y + 1\rangle$, de (3.18) en el corolario 3.11

$$\eta^{2^{e-3}\cdot 3} = 1 + 2^{e-1}\left(h_1\eta + h_2\right)$$

con $h_1 \equiv 0 \pmod 2$ y $h_2 \equiv 1 \pmod 2$.

Sustituimos en la ecuación (3.23), y se tiene

$$2^{e-1}\left(h_1\eta + h_2\right)\left(\left(1 + 2^{e-1}\left(h_1\eta + h_2\right)\right)(3\eta - 1) - 1\right) = 0$$

desarrollando y considerando $h_1 \equiv 0 \pmod 2$ y $h_2 \equiv 1 \pmod 2$ queda

$$2^{e-1}\cdot 3h_2\eta = 0$$

por lo tanto existen $u_1(y), u_2(y) \in \mathbb{Z}[y]$ tales que

$$2^{e-1}\cdot 3h_2\eta = u_1(y)(y^2 - uy + 1) + 2^e u_2(y)$$

lo que implica que $h_2 \equiv 0 \pmod 2$, que es una contradicción.

Por lo tanto $k \notin K_e$.

□

3.4. El grupo G_n

Sea $n = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Para poder utilizar los resultados de las 3 secciones anteriores es necesario considerar las siguientes posibilidades:

1. $e < 3$, para el cual se calcula $v(n)$ como ya se definió antes y se sabe que $D_k(x)$ es un polinomio de permutación de Dickson si y sólo si $(k, v(n)) = 1$.

2. Si $e \geq 3$, definimos $w(n) = \left[3 \cdot 2^{e-2}, p_1^{e_1-1}\left(\frac{p_1^2-1}{2}\right), \ldots, p_r^{e_r-1}\left(\frac{p_r^2-1}{2}\right)\right]$ y también se tiene $D_k(x)$ es un polinomio de permutación de Dickson si y sólo si $(k, w(n)) = 1$.

Proposición 3.20. *Sean $e < 3$ y $k \equiv l$ (mód $v(n)$), entonces $D_k(u) \equiv D_l(u)$ (mód n) para todo $u \in \mathbb{Z}$. Y si $e \geq 3$, sea $k \equiv l$ (mód $w(n)$), entonces $D_k(u) \equiv D_l(u)$ (mód n) para todo $u \in \mathbb{Z}$.*

Demostración. Sea $e < 3$, como $k \equiv l \pmod{v(n)}$, entonces $k \equiv l \pmod{3 \cdot 2^{e-1}}$ y $k \equiv l \pmod{p_i^{e_i-1}\left(\frac{p_i^2-1}{2}\right)}$ por el teorema 3.5 y la proposición 3.15 se tiene que $D_k(u) \equiv D_l(u) \pmod{2^e}$ y $D_k(u) \equiv D_l(u) \pmod{p_i^i}$ para todo $u \in \mathbb{Z}$. Utilizando el teorema chino del residuo $D_k(u) \equiv D_l(u) \pmod{n}$ para todo $u \in \mathbb{Z}$.

Ahora supóngase que $e \geq 3$ y $k \equiv l \pmod{w(n)}$, entonces $k \equiv l \pmod{3 \cdot 2^{e-2}}$ y $k \equiv l \pmod{p_i^{e_i-1}\left(\frac{p_i^2-1}{2}\right)}$ por el teorema 3.5 y la proposición 3.17 se tiene que $D_k(u) \equiv D_l(u) \pmod{2^e}$ y $D_k(u) \equiv D_l(u) \pmod{p_i^i}$ para todo $u \in \mathbb{Z}$. Por el teorema chino del residuo $D_k(u) \equiv D_l(u) \pmod{n}$ para todo $u \in \mathbb{Z}$. □

Proposición 3.21. *Si $e < 3$, entonces la función ψ definida como:*

$$\psi : \mathbb{Z}^*_{v(n)} \to G_n$$

$$\psi(k) = D_k(a)$$

es un epimorfismo.

Si $e \geq 3$, entonces la función ψ definida como:

$$\psi : \mathbb{Z}^*_{w(n)} \to G_n$$

$$\psi(k) = D_k(a)$$

es un epimorfismo.

Demostración. La demostración es idéntica a la del corolario 3.6. □

Considérese ahora el núcleo $Nu(\psi) = K_n$ del epimorfismo ψ. Sea $\overline{k} \in K_n$, entonces tenemos $D_k(a) \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$; así que tenemos $k \bmod p_i^{e_i-1}\frac{p_i^2-1}{2} \in K_{p_i^{e_i}}$ y

k mód $2^{e-1} \cdot 3 \in K_{2^e}$ para $e < 3$ y k mód $2^{e-2} \cdot 3 \in K_{2^e}$ para $e \geq 3$. Pero ya que si m es el mínimo común múltiplo de los números $\ell_1, \ell_2, \ldots, \ell_r$ la imagen de

$$k \text{ mód } m \to (k \text{ mód } \ell_1, k \text{ mód } \ell_2, \ldots, k \text{ mód } \ell_r)$$

es un monomorfismo μ del grupo $\mathbb{Z}_m^*$ en el producto directo de $\mathbb{Z}_{\ell_i}^*$, así K_n es isomorfo a un subgrupo de $K_{2^e} \times K_{p_1^{e_1}} \times \cdots \times K_{p_r^{e_r}}$.

El orden de K_n depende de la naturaleza de la descomposición en factores primos de n. No es fácil encontrar una fórmula general para ello, pero en [11] se hacen las siguientes afirmaciones, cuyas demostraciones pueden consultarse ahí mismo.

Teorema 3.22. *Si los exponentes de todos los factores primos $p_i > 3$ de n son mayores que 1, entonces K_n tiene orden 2, con la excepción de los casos $n = 6, 12, 24$ donde tiene orden 4.*

Teorema 3.23. *Sea o el orden de K, y supóngase que en la descomposición de n en factores primos se tiene que el número primo 2 está a lo más a la tercera potencia, 3 como máximo a la primera potencia, y de lo contrario aparecen sólo primos $p \equiv \pm 5$ mód 12 a la primera potencia, entonces $2 \leq o \leq 4$. En todos los demás casos para n se tiene $2 \leq o \leq 2^{1+r}$ si r es el número de factores primos de n con exponente 1 y $p_i \equiv \pm 1$ mód 12.*

Como consecuencia de la proposición 3.20 se puede demostrar el siguiente teorema que es el resultado que se persigue en este capítulo, y con esto se tiene que $D(n)$ es un grupo abeliano:

Teorema 3.24. *Si la permutación π es inducida por un polinomio de Dickson $D_k(x)$, entonces la permutación π^{-1} es también inducida por un polinomio de Dickson $D_t(x)$, tal que $kt \equiv 1$ (mód $v(n)$).*

Demostración. Sea π una permutación inducida por el polinomio de Dickson $D_k(x)$, entonces $D_k(x)$ es un polinomio de permutación módulo n y por el teorema 2.12 $(k, v(n)) = 1$ por lo que existe $t \in \mathbb{Z}_{v(n)}^*$ tal que $kt \equiv 1$ (mód n). Así $(t, v(n)) = 1$ y por el teorema 2.12 se tiene que el polinomio de Dickson $D_t(x)$ es un polinomio de permutación módulo n. Y para que la permutación π^{-1} sea inducida por el polinomio de Dickson $D_t(x)$ es necesario que $D_k(D_t(x)) = D_t(D_k(x)) \equiv x$ (mód n), pero $D_1(x) = x$ y por el lema 3.1 sólo hay que mostrar que $D_{kt} \equiv D_1(x)$ (mód n). Esto sucede por la proposición 3.20 ya que $kt \equiv 1$ (mód n). □

Se ha demostrado que G_n es un grupo, y además $D(n)$ es equivalente a G_n, trivialmente, sólo que uno es expresado como polinomios y el otro como permutaciones.

Del corolario 3.6 se tiene que $\psi : \mathbb{Z}_m^* \to G_{p^e}$ dada por $\psi(k) = D_k(a)$ es un epimorfismo (donde $m = p^{e-1}(p^2 - 1)/2$), y por lo anterior es un isomorfismo de grupos. Por el

teorema fundamental de homomorfismo $G_{p^e} \cong \mathbb{Z}_m^*/Nu(\psi)$. Luego G_{p^e} tiene cardinalidad $\varphi\left[p^{e-1}(p^2-1)\right]/2/|Nu(\psi)|$, donde φ es la función de Euler.

Así

$$|G_{p^e}| = \begin{cases} \varphi(p^2-1)/8, & \text{si } p \geq 5 \text{ y } e = 1 \\ \varphi\left[p^{e-1}(p^2-1)\right]/4, & \text{si } p \geq 5 \text{ y } e > 1 \\ 1, & \text{si } p = 3 \text{ y } e = 1 \\ 2 \cdot 3^{e-2}, & \text{si } p = 3 \text{ y } e > 1 \\ 1, & \text{si } p = 2 \text{ y } e = 2 \\ 2^{e-3}, & \text{si } p = 2 \text{ y } e > 2 \end{cases}$$

Capítulo 4

Cifrado de Dickson

Este capítulo explica una aplicación de los polinomios de Dickson a la criptografía, que es un sistema de cifrado basado en ellos. Antes de describir en qué consiste el esquema de cifrado basado en los polinomios que son objeto de estudio de este trabajo, se explican algunos algoritmos que son de gran utilidad para evaluar eficientemente un polinomio de Dickson.

Algunos resultados de los capítulos anteriores nos sirven para describir un esquema de cifrado basado en polinomios de Dickson (cf. [19]) con parámetro $a = 1$, aunque también se dan de manera similar esquemas de cifrado basados en polinomios de Dickson con parámetro $a = -1$ (cf. [20]). El primer caso es uno de los objetivos más importantes de este trabajo.

4.1. Algoritmo de evaluación rápida para polinomios de Dickson

Ahora se da un algoritmo de evaluación de complejidad $O(\log(k)\log^2(n))$, donde k es el grado del polinomio de Dickson y n es el módulo al que se reduce $D_k(x)$, el cual permite calcular los valores de la función $D_k(x)$ mód n.

Queremos calcular $D_k(b)$ mód n, para hacer esto se resuelve

$$u + \frac{1}{u} = b \tag{4.1}$$

o equivalentemente

$$u^2 - bu + 1 = 0 \tag{4.2}$$

en alguna extensión del anillo $\mathbb{Z}_n$. Si (4.2) no tiene solución en $\mathbb{Z}_n$, entonces la solución está en $R_b = \mathbb{Z}_n[u]/\langle u^2 - bu + 1\rangle$, una extensión del anillo $\mathbb{Z}_n$, y cada elemento $s \in R_b$

puede representarse de forma única como

$$s = a_1 u + a_0 \text{ con } a_1, a_0 \in \mathbb{Z}_n$$

La multiplicación en R_b puede ser implementada considerando que $u^2 = bu - 1$ y usando la fórmula

$$\begin{aligned}(a_1u + a_0)(b_1u + b_0) &= a_1b_1u^2 + a_1b_0u + a_0b_1u + a_0b_0 \\ &= a_1b_1(bu - 1) + u(a_1b_0 + a_0b_1) - a_0b_0 \\ &= (a_1b_1b + a_1b_0 + a_0b_1)u + a_0b_0 - a_1b_1.\end{aligned}$$

Por lo tanto $(a_1u + a_0)(b_1u + b_0) = (a_1b_1b + a_1b_0 + a_0b_1)u + a_0b_0 - a_1b_1$.

Obviamente, los elementos $u, u^{-1} \in R_b$ son solución de (4.2). Como $u(b - u) = 1$, se tiene que u siempre es invertible.

Ahora para la evaluación de $D_k(b)$ calculamos la potencia u^k en el anillo R_b usando el algoritmo de elevar al cuadrado y multiplicar, que se muestra a continuación:

Algoritmo 1.

Entrada: n, k, b
Salida: $d = a_1u + a_0 = (u^k \mod u^2 - bu + 1) \mod n$
1. Calcular $\{c_m, c_{m-1}, \ldots, c_1, c_0\}$ tal que $k = \sum_{i=0}^{m} c_i 2^i$.
2. $c \leftarrow 0$.
3. $d \leftarrow 1$.
4. Para $i = 0$ hasta m
    4.1 $c \leftarrow 2c$
    4.2 $d \leftarrow (d^2 \mod u^2 - bu + 1) \mod n$
    4.3 Si $c_i = 1$
        4.3.1 $c \leftarrow c + 1$
        4.3.2 $d \leftarrow (d * u \mod u^2 - bu + 1) \mod n$

El número de pasos requeridos para este algoritmo es $O(\log(k)\log^2(n))$, pues depende de la expresión en binario de k, y puede programarse en Mathematica como muestra a continuación:

```
Potencia[n_, k_, b_] := Module[{c},
  d = 1;
  c = 0;
  Lista = IntegerDigits[k, 2];
  a = Length[Lista];
  For[i = 1, i <= a,
   c = 2*c;
   d = PolynomialRemainder[d^2, u^2 - b*u + 1, u];
```

```
  d = PolynomialMod[d, n];
  If[Lista[[i]] == 1,
   c = c + 1;
   d = PolynomialRemainder[d*u, u^2 - b*u + 1, u];
   d = PolynomialMod[d, n];
   ];
  i++];
 d
 ]
```

Con el algoritmo 1 encontramos elementos $a_0, a_1 \in \mathbb{Z}_n$ tales que $u^k = a_1u + a_0$. Además se tiene que $\frac{1}{u}u + \frac{1}{u}\frac{1}{u} = \frac{1}{u}b$ por lo que

$$(u^{-1})^2 - b(u^{-1}) + 1 = 0 \tag{4.3}$$

y así u^{-1} también satisface (4.2). De esta manera despejando u^2 y $(u^{-1})^2$ de las ecuaciones (4.2) y (4.3), respectivamente se obtiene

$$\begin{aligned} u^2 &= bu - 1 \\ (u^{-1})^2 &= b(u^{-1}) - 1 \end{aligned} \tag{4.4}$$

De estas dos igualdades se puede demostrar la siguiente proposición:

Proposición 4.1. *Sea $k \geq 2$, entonces se cumple que en el anillo R_b existen $a_1, a_0 \in \mathbb{Z}_n$, calculados con el algoritmo 1, tales que $u^k = a_1u + a_0$ y $u^{-k} = a_1u^{-1} + a_0$.*

Demostración. Se procede a hacer la demostración haciendo inducción sobre k.

Para $k = 2$ se cumple, pues en la ecuación (4.4) se considera $a_1 = b$ y $a_0 = -1$.

Si $k = 3$, se calcula

$$\begin{aligned} u^3 &= (bu - 1)u = (b^2 - 1)u - b \\ u^{-3} &= (b(u^{-1}) - 1)u^{-1} = (b^2 - 1)u^{-1} - b \end{aligned}$$

por lo que se toman $a_1 = b^2 - 1$ y $a_0 = b$, y así se satisface la proposición.

Supóngase que la propiedad se cumple para $k = t$, entonces existen $d_1, d_0 \in \mathbb{Z}_n$ tales que $u^t = d_1u + d_0$ y $u^{-t} = d_1u^{-1} + d_0$.

Calculando u^{t+1} y $u^{-(t+1)}$, se obtiene:

$$\begin{aligned} u^{t+1} &= (d_1u + d_0)u = d_1(bu - 1) + d_0u = (d_1b + d_0)u - d_1 \\ u^{-(t+1)} &= (d_1u^{-1} + d_0)u^{-1} = d_1(bu^{-1} - 1) + d_0u^{-1} = (d_1b + d_0)u^{-1} - d_1 \end{aligned}$$

tomando en cuenta a $a_1 = d_1b + d_0$ y $a_0 = -d_1$ se obtiene el resultado deseado. □

Como consecuencia de la proposición 4.1 se satisface la siguiente igualdad

$$D_k(b) = D_k(u + \frac{1}{u}) = u^k + \frac{1}{u^k} = a_1 u + a_0 + a_1 \frac{1}{u} + a_0 = a_1(u + \frac{1}{u}) + 2a_0 = a_1 b + 2a_0$$

con la que se tiene una forma de evaluar rápidamente un polinomio de Dickson, el procedimiento se resume en el siguiente algoritmo:

Algoritmo 2.
Entrada: n, k, b **Salida**: $D_k(b)$ 1. Calcular $a_0, a_1 \in \mathbb{Z}_n$ con el Algoritmo 1. 2. Calcular $D_k(b) = a_1 b + 2a_0$ mód n.

El algoritmo puede programarse en Mathematica como:

```
dicksonpol[n1_, k1_, b1_] := Module[{pol, as, a0, a1, gk},
  pol = Potencia[n1, k1, b1];
  as = CoefficientList[pol, u];
  a0 = as[[1]];
  If[Length[as] == 1,
   a1 = 0;,
   a1 = as[[2]];
   ];
  gk = Mod[a1*b1 + 2*a0, n1];
  gk
  ]
```

4.2. Cifrado de Dickson

Uno de los criptosistemas de llave pública más importante es el sistema de cifrado RSA (ver el apéndice A). El RSA satisface la propiedad de que el texto en claro y el texto cifrado están en el anillo $\mathbb{Z}_n$, y la función de cifrado es de la forma x^k, la cual es un polinomio de permutación. Existen variantes del RSA en el que se cambia el grupo de permutaciones, que son potencias, por algún otro grupo de polinomios de permutación, uno de ellos es el que presentaron Muller y W. Nobauer en 1981 (cf. [18]), está basado en polinomios de permutación de Dickson y se describe a continuación. A este esquema se le llama *cifrado de Dickson.*

Cada participante P de la red de comunicación elige un entero positivo $r_P := r$, donde r será el número de factores $p_i^{e_i}$, con cada p_i primo impar (mayor que 10^{80}), del módulo n; y una llave de cifrado $k_P := k$ con $(k, p_i^{e_i-1}(p_i^2 - 1)) = 1$, para cada $1 \leq i \leq r$.

Entonces P calcula los siguientes números:

$$n_P := n = \prod_{i=1}^{r} p_i^{e_i}$$

$$v(n) = \left[p_1^{e_1-1}(p_1^2-1), \ldots, p_r^{e_r-1}(p_r^2-1)\right]$$

y también calcula la llave de descifrado $t_P := t$, tal que $t \in \mathbb{N}$ satisface la congruencia

$$kt \equiv 1 \text{ (mód } v(n)). \tag{4.5}$$

La llave pública de P consiste de los parámetros n_P y k_P, y la llave secreta está dada por la factorización en primos de n y por t_P.

Supóngase que A desea enviar un mensaje m a B, al que se denomina texto en claro, para esto tanto A como B tienen sus llaves públicas $n_A,\ k_A,\ n_B,\ k_B$ y llaves secretas $t_A,\ t_B$, respectivamente; así que el mensaje m se elige de tal manera que $m \in \mathbb{Z}_{n_B}$.

A cifra el mensaje calculando:

$$c \equiv D_{k_B}(m) \text{ (mód } n_B),$$

y envía c a B. Llamamos a c el texto cifrado correspondiente al mensaje m.

Cuando B recibe c, para encontrar m realiza lo siguiente:

$$D_{t_B}(c) = D_{t_B}\left(D_{k_B}(m)\right) \equiv m \text{ (mód } n_B).$$

Ejemplo 6. Supóngase que B elige $n_B = 13^2 \cdot 11^3 \cdot 7^5 = 3780549773$, y calcula $v(n_B)$ que resulta ser $v(n_B) = 906425520$. Enseguida elige aleatoriamente un número en $\mathbb{Z}^*_{v(n_B)}$ como llave pública digamos $k_B = 4433549$. De aquí el valor de t_B tal que $k_B t_B \equiv 1$ (mód $v(n_B)$) es $t_B = 521531669$, el cual se calcula utilizando el algoritmo extendido de Euclides.

De este modo la llave pública de B es $(3780549773, 4433549)$.

Si A desea enviar el mensaje $m = 745312659 \in \mathbb{Z}_{n_B}$ al usuario B, cifra el mensaje calculando $D_{4433549}(745312659)$ mód 3780549773 para lo que utiliza el algoritmo 2, con lo que obtiene el mensaje cifrado

$$c \equiv 2499970564 \text{ (mód } 3780549773),$$

el cual se envía a B.

Al recibir el mensaje cifrado B emplea su llave secreta t_B para calcular

$$D_{521531669}(2499970564) \quad \text{mód } 3780549773,$$

usando también el algoritmo 2. El resultado es $d \equiv 745312659$ (mód n), que corresponde al mensaje original m.

Utilizando Mathematica se implementó una función con la que se pueden cifrar mensajes utilizando el sistema de cifrado basado en polinomios de Dickson, que se ha descrito en esta sección.

La función recibe como entrada un mensaje m y devuelve como salida el mensaje cifrado c, el valor de n y la llave de cifrado k, de la siguiente manera: elige aleatoriamente dos números primos, cuyo producto es n, calcula $v(n)$ para poder elegir aleatoriamente la clave de cifrado k.

En la práctica se recomienda que los números primos sean mayores a 10^{80}, y en este caso la función elige los números primos entre 10^{80} y 10^{90}, quedando implementado de la siguiente manera:

```
cifradodickson[m_] := Module[{n, p1, p2, a, k1, k, gc},
  p1 = RandomPrime[{10^80, 10^90}];
  p2 = RandomPrime[{10^80, 10^90}];
  n = p1*p2;
  a = LCM[p1^2 - 1, p2^2 - 1];
  k = RandomInteger[a];
  gc = GCD[k, a];
  While[gc != 1,
   k = RandomInteger[a];
   gc = GCD[k, a];
   ];
  Print["n = ", n, "\n k = ", k];
  Print["El mensaje cifrado es: ", dicksonpol[n, k, m]];
  ]
```

Se muestra un ejemplo del uso de esta función:

Ejemplo 7. El mensaje a cifrar es $m = 36244283562354371$, obteniendo como salida:

$n =$ 93185119958620172374550651641295809666369852418877898724429596605261972080375736193270721477883149400975229299997123533729637669331764623960118574930250539239917580661802240264004025048861917595161 09

$k =$ 64103388982289304325830082284725301040222568976936759944922289280970301475887374516897492175739977439403619833884686149030015740380812824714358942782956516943040616588470655514396584042855323465716050271205694588526355454862912145497215531012902311611377731061682926410868136881930487616237357497127670121919036685891488429951272521882611497490130617865000115479292582009546950383665448703833736 5

y el mensaje cifrado es:

$c = 872578661493739209485882290803614029574103414100298476852656279498993$
$340332636128564171425535794599412437778151499203928063770619681422050622386956$
$622125649373793060917895218736408420260221436208888$

Para descifrar se calcula la llave de descifrado, que es:

$t = 440042512744227573431142234304740945665268624151266540629580082054004871$
$780246632527694608525496262464883505923659918964090550189516579398906253342$
$497482614614900649711221858996866382628826149862070764036632133271902327324844$
$955664518776134975285887489985984488178909672371704999289033157093107446020006$
$282941225011433545695966522279154720299500574992884005798681634985266255058011$
965154396642845

y al calcular $D_t(c)$ mód n resulta: 36244283562354371, que corresponde al mensaje original.

Se evaluó la función cifradodickson[m] en SAGE para varios valores de m en todos ellos el tiempo de ejecución fue menor a 1 segundo.

En el apéndice D, se muestran los algoritmos de esta sección implementados en SAGE.

4.3. Comparación con RSA

En esta sección se muestra una comparación de los tiempos de ejecución al cifrar mensajes con RSA y el cifrado de Dickson.

La implementación del sistema de cifrado de Dickson se realizó primero con el software Wolfram Mathematica 9.0, posteriormente con SAGE. Con este último se logró un mejor rendimiento en cuanto a los tiempos y mayor cantidad de dígitos a considerar para el cifrado. Por esta razón se utiliza SAGE en los cálculos que se muestran a continuación.

Para todos los cálculos se usó una computadora con las siguientes características:

- Procesador: Intel(R) Core(TM)i5-2467M CPU @ 1.60GHz 1.60GHz
- Memoria (RAM): 4.00 GB

Se comparan los tiempos de ejecución al cifrar un mensaje m con el sistema de cifrado basado en polinomios de Dickson (t_D) y RSA (t_{RSA})(implementaciones con SAGE). Para el cifrado de Dickson se emplean los algoritmos 1 y 2, para RSA se utilizan los que se muestran en el Apéndice A.

Para los valores de los mensajes se consideraron de tal manera que fueran de diferente número de dígitos. La elección de los números primos se hizo de manera aleatoria entre 10^{180} y 10^{200}.

Al final de la sección se muestran los valores de los primos p y q, las llaves de cifrado e y k para RSA y cifrado de Dickson, respectivamente, además del mensaje cifrado c en ambos casos, para cada uno de los mensajes m_i.

SAGE utiliza los conceptos de CPU time y Wall time , que son los tiempos que el ordenador dedica exclusivamente a nuestro programa. El CPU time es el tiempo de CPU que se ha dedicado a nuestro cálculo, y el Wall time el tiempo de reloj entre el comienzo y el final del cálculo.

mensaje	t_D	t_{RSA}
m_1	CPU 0.52 s, Wall: 0.94 s	CPU 0.02 s, Wall: 0.03 s
m_2	CPU 0.53 s, Wall: 0.93 s	CPU 0.02 s, Wall: 0.03 s
m_3	CPU 0.52 s, Wall: 0.92 s	CPU 0.02 s, Wall: 0.06 s
m_4	CPU 0.54 s, Wall: 0.94 s	CPU 0.02 s, Wall: 0.03 s
m_5	CPU 0.57 s, Wall: 1.04 s	CPU 0.03 s, Wall: 0.05 s

Cuadro 4.1: Tiempos de ejecución del cifrado de Dickson y RSA.

De la tabla se puede notar que el mensaje m se cifra más rápido con RSA que con el sistema de cifrado de Dickson, aunque la diferencia no es mucho.

Para el sistema de cifrado de Dickson no importa el número de dígitos del mensaje m y los números primos p y q, pues el tiempo de ejecución de los ejemplos es alrededor de 1 segundo, lo cual se debe al algoritmo de evaluación rápida que se describe en la sección 4.1.

Con RSA mientras más grandes son los valores de los números primos p y q el tiempo de ejecución es casi el mismo. Considerando que en la actualidad el orden de los números debe ser alrededor de 10^{200}, resulta que el sistema basado en polinomios de Dickson es ligeramente más lento que RSA.

Mensaje $m_1 = 56$

```
El mensaje original es:  56
p =
676247637510000717729515196331825566305035127850469120674570884728927842\
286670539304126236993781758873249416106748644188425799520069044039431353\
40849601327581142913687903745842658 3
q =
864852565384558686746147013400291335387344325013786069798792569319795976\
092574187828876133303219123276393596095843670580075965272772024428516852\
318097896610918412924403899966484357
n =
584854504135771237276242536670267062503034916021536055287140578139512740\
392140939588748689607989066958771754618120853059441302649260650330404167\
```

```
861566143546945268045535471842001839093042965362081489418465486576614174\
527386474985345548144582086825875271145919120424756109027754965991538207\
871966673870811658634488134984825946933789111765490381235233447302462131

Resultados del cifrado de Dickson
vn =
142522829586624523036566711836459774868037061694885342586041741424211034\
141894036190096481625828647285579458100647077228150656984978716424435188\
134869679865364479804877940405076403041121038492060258925895333896566544\
490355186082742906567362660631309413299890186847327369037984985789250353\
719718630988111292340585618051224591299619630843623392779068853876461592\
088736232150004592093544429070274523667408753549725036365126354834994063\
112683718366519727357724667625656666727493836881690865485492593550860597\
796261559387983127579240665945638241074697094591300990120395476752523533\
291999109071997048616998551015547017614680889182486973538300423783061603\
192887655680372788559595149728745692320989812606390126238471034317625 76
k =
103623728433682650522157292980634523111150249417656673642579545216925443\
355609621347377630476475213300933703290385441101342849536807999099299496\
455769812795102197144498535706491648720898651793830022943028092874343761\
989933485141870810791661709905701570984075979563123317971693187861591792\
251208919773395013404513542400787010343419481657596993377655006416640234\
492074423605276222776051151172308011011171286910614070441964100740128023\
890499478969738684337290721746782752193600755117501648346219964248679483\
540351654641512089444514175528043288190758919436098586145085481542691035\
724029078857944813070224848312338863620419482978176649760240270016030756\
828604174364804187960934219176659219777325764615785945864059594972271 59
El mensaje cifrado con el sistema de cifrado de Dickson es c =
667247831009545746187024509780996597617238571056521241476422972295894949\
920416410168811345849052842062220006837625510260698863497434749006864032\
147983204224512517218752744007177042136327967511980999134714227180000840\
311225886300458734848602746320148681018733801902911600819740289644414244\
898697748592822282836280817868563353099044937943535871099981405652475 29
Time: CPU 0.52 s, Wall: 0.94 s

Resultados de RSA
phi(n) =
584854504135771237276242536670267062503034916021536055287140578139512740\
392140939588748689607989066958771754618120853059441302649260650330404167\
861566143546945268045535471842001837551942762467522084942803276844497272\
835007022121090357671218632777151452766674393291753738730754083841895195\
```

```
669374359102309893841647066516877741207195201878760539173950509877551192
e =
184445194944352155537898855441610561791332539789260208984154346769278973\
516912656680144794657142207873375953288567006202932241382717430017161545\
798706188457655750450815140343855295604563749629860856521839733715590884\
654716835736033939601408247553732196869061824750558839043096371725956369\
500605371697789629572467085066518576294579347445551671653756279492730003
El mensaje cifrado es:
439543420167728410357490118673387279380159556179932758109573116579090674\
711088927824964240250382730162672492858330557043352191466918453848880077\
898898238430284681147317112667180092925689675366054469025986101008138547\
067315368307613679437152045429584230688436767868884482322071925168039480\
444796058884535269415084441790809182854509743881904102796223237318094988
Time: CPU 0.02 s, Wall: 0.03 s
```

Mensaje $m_2 = 234425643$

```
El mensaje original es:  234425643
p =
363789983742500776223306950695641616151884212036182653585630026760230380\
540987130882887968065659863419999423155088347086206578841483150129780945\
010899923126017100548923413568815913
q =
497385496003650514923802194262105779383224203667872166878531429388712210\
208955357666878752440088233117057989271614662939851634035248329481979355\
392718603510326598202558019776632479
n =
180943861504923705626996291142511304780190912767197077975581902927631740\
360737663635163115819430115254760177654344376655229813044057562753811169\
179111150994229878939121824465614390862708615297015372832111484109671513\
652208770901178704038290312681994433659541233005884665488801768245944054\
268053641876501269674577856091604963492232232200473696974048086607838327

Resultados del cifrado de Dickson
vn =
682097521173187726418754541835620823523881901685059989644575536919622985\
527985282362519466905998477898045932934502991303751404931389056426895333\
377970726766558768349858643230714758067581533266621881090928373280403529\
811525487174537223928576800281131717051568666270016562567152873775256564\
666928499476152220061037270566245462593632811601749450245289423537853295\
931815368915237652175028671320494564636414587035046947752171241043588301\
696650573200195694439855942549939113267833738840720065164591169479716015\
```

```
95397806917220328740011494629043868011366984309061236887004927942444717 8\
55525188767912874607453098173078580810910884766791072159684661091303305 4\
83132321003396652931741137682899400087995333882988887346670386355104 0
k =
31811197978369204081198040179124895363212845414510036094289345601380875 2\
24941736727542749756359325762351518041962812391704204061263231382233698 0\
20030472684798229365529409403388274503836802646534602078155065724849530 0\
59444226941315219744324025946880913641025165517620942166315868546358212 2\
69308362800550978087216446861039516290687383920934007757723489905311220 \
88214259294105037161143891068073534340440097357478767293276517626522891 7\
38608805970451522631991510633752225102422757219750797987679072333658419 1\
12676637348652519735552035907596595986120694706862530850584871667201900 6\
03020171086246969949044613825192742907318232702057229832615700075083168 0\
72018324921349523007091834720812766055345935023704200580613037912231 7
El mensaje cifrado con el sistema de cifrado de Dickson es c =
13844913829242751821515649065914393713679349105222378998081046677307532 2\
65003496341258127089580880402886335668202857438201487066772188934581093 0\
34222084245986837018573561878096856976204880123506350328961013744824901 7\
19950114000357765929962514618952940545844503613772147807627704331232564 1\
15543242225265163539943701661254216124965561093807958066925926376784310 4
Time: CPU 0.53 s, Wall: 0.93 s

Resultados de RSA
phi(n) =
18094386150492370562699629114251130478019091276719707797558190292763174 0\
36073766363516311581943011525476017765434437665522981304405756275381116 9\
17911115099422987893912182446561439000153313555086408168500233915192411 8\
11710035519712388357412885653305184290959874445611794498305367170888664 1\
84135063185044305679784637647984466308861370556412999822256665326238993 6
e =
30209829753784722595282448984192421016943904210790733036302343411395572 6\
50644884737072112180417630998153146081254289286182217933085684903555235 4\
05820396837014923534452193072262403003769305303678993726536842941260235 5\
15255255002327168306740388491821149314770309803071888441871142873985048 4\
92912342388914357938486930424373075061516268995887659029554585666976757
El mensaje cifrado es:
97191990691630727315083949856390808994532382579383430647067209878091791 7\
03159495907456798713841886154924489505231912863071149074822919008860408 5\
61230531456707878149998685161905503655858476294420800211491745687951063 3\
58036656264722562111048927934093686941712129816194145275136129029993732 8\
19264897656120456739528094500661296704321427143512030395737917124773010
```

```
Time: CPU 0.02 s, Wall: 0.03 s
```

Mensaje $m_3 = 345265471253812751747123623564234 72$

```
El mensaje original es:  345265471253812751747123623564234 72
p =
816398940746433725238253056435583963741410992843297125242383632947910034\
149892768645749888669177674944503964830421497729106185629864345818671855\
168922720655523359803585430170635223
q =
160877441148215007178066451749434413571965509667411320461877296776018424\
490784839144736793194132669087083068194807695564638566255310490241815393\
517378573844860363274340127654790119
n =
131340172543399462455325789431723288613688686645609243694919703728104713\
723540280204676249608369903644962502129370529265863651744706380752809985\
131166698464567741486519130922764900632864178340201467477145656322462502\
765512329037366043329281254652033844289376659189189622210426105710086752\
620388667001933391227326299479130307554567026185797168196589748973761537

Resultados del cifrado de Dickson
vn =
119793339748124597378215547199539306923778078956230373351199076567771326\
943689464850862348718008282066563021671260086995258423180388109298308689\
748656014929139558886739904206653497093809212694252756920399052559985733\
612286018547397146472768327193883115444684522771220211877108161530529245\
101553939801991648619680103715569706468128384226453163089034321387322902\
848702149915782072847722562638926940975475173059671417710134350415754958\
570801002277047192785230016560939940079405068680078547897298904006993709\
350214325331521588999583008553955027686252776199940503248290896372328350\
636216083621849052763461922312441350809122355461914397252562875233546478\
729058780009213379128824350460701183871648497205521548106794428279920
k =
113252688157409976075593420193345249914587922827240373408608923757302573\
037937025044364028825396601616288271825617475319583988788013510225438998\
740375372922013028795486663988612736903682610075772034040515266200326814\
583597025256476081272176452571323087988263432085430266548566720537735075\
109220059393317023599567729017266425702950985935161936819662573806969179\
077419575337912020484963074274264039455485385937572887571804669101679975\
387109093620090074715366190405673605883861561931142755925280701202891768\
649302149564200972829551508042332982127943502469664992408157549332119418\
317100304140011732473146215285232313826088300668657320330037373642207745\
```

```
944527775937537884054323550397107725702017201304290009582220046762951
El mensaje cifrado con el sistema de cifrado de Dickson es c =
976135134099644717701793625995483135168364157763936509272959405442898444\
103939656375766807391504365654603272423984281505529081700075074951380419\
323350033474725378702267174438648907519572960466880205037363947505832299\
668733675123454177767154852354705499401981082095393283574142649347755482\
238306434109620843632652557568101456041104031323408912519123226597436 31
Time: CPU 0.52 s, Wall: 0.92 s

Resultados de RSA
phi(n) =
131340172543399462455325789431723288613688686645609243694919703728104713\
723540280204676249608369903644962502129370529265863651744706380752809985\
131166698464567741486519130922764899655587796445552735060826148137444125\
452135826526657597625020324928105385648699051398702940347115761678499719\
595159473708188639342151463418643058868265731685413445118664191148336196
e =
120815770491331012356668018278480998282861798747337312068531307762668194\
413969929522906731209174523301499515906214460339041388797120009823205727\
995629992780545531519270064212891737437544904590970792174401864957687236\
740488815970356875802263658850998234653936761211281508439969842556813012\
800900499447944462830933440329200469624238531663674968283312923220757 43
El mensaje cifrado es:
199731100644475745182214748417514743651420181900322918430415114895021451\
965041217334825199996003007715077211561419795205565641426892030295363470\
649718183614545544173973976046022432023377778824346225401869272065001726\
053076058390323716171959298405613681490157674030833458242069862802898265\
489707033192926135364191923868920800681548597222651099927726511657572 62
Time: CPU 0.02 s, Wall: 0.06 s
```

Mensaje $m_4 = 934238565234523843752385428734132454534535542 13$

```
El mensaje original es:  934238565234523843752385428734132454534535542 13
p =
488153850856344575998736510300712277983355553317377723137512506521230241\
559539912702570861537489572687674096249717467784226509934439674810909521\
501630011424159588587550840214986769
q =
862328398541032082000865429587748685914877994147111527812507150370923151\
847203600948483817620829521534833796569526639155218001067902889633067229\
494679501317683722511491016882980353
n =
```

```
420948928450589440622527756599631900264892349693029281297917230737847393\
694952758792056221851973205363997729970298101287180113772935641843325314\
077527667026960256083814437816088177664480682813391770323255789365194733\
768053762966834683054861002313433712563419873974606036377985907382949457\
185614815378920271705068240142660714869733396429261871200842917181949457

Resultados del cifrado de Dickson
vn =
184581250378853612707683612064835847990758743028459937544027897123058787\
236805189672593600585956594603235169552065113447932770629761412960733154\
430157999727185431941221489174579437096263715520276207180696125528289283\
620626815955025122450546786973001018811944835547603802897758063153531051\
966603088183310018103923235925039639996488681893132383868751689793636656\
014725860453519338167052776136590373322575507958428773515406998271699958\
323295216994737698493728993455653817887491238355738644637711869162832214\
398171827256054240469899574682470754724882553482253710232296658154036171\
287872674148885911842323036763270382549220823668117656547070195578081897\
167129795348020265780777656646590482749116851202636687948369700284928 0
k =
453467243718495295879548767692294473055452408314382132421568812594176295\
745888206498625884656014775876596099622517011202314614229075408437766556\
323645130176291394607190479413173046441464366074615690613190747626444705\
325088092538484026742011150269459602445453635158410643842803721001238741\
214368990868294390298522812407635647719715815220956768654367745882186931\
320775509464170752955986392075477911054191094583952970363865637519474290\
588805808653156625188296080767239007959117618179415175031988270881395873\
641737382181976483248523894725381426987534429705067564808680190947802932\
735559557923800179210944428881666794607810750294385630282152431114378411\
612481433363380364007637693667214397110228608830292074399413479514849
El mensaje cifrado con el sistema de cifrado de Dickson es c =
259836519766484267281789017035316809621439869614717260306930025662450809\
112232926057619223576829076052215442455498191204648937408946473586059839\
473379425058216139218968378589061152612948157474724068146722829711043473\
048013631938862586370900190051159168610936256061030876911242400746546534\
631110398095964590595867375877616925911100405311328239910426945373951997
Time: CPU 0.54 s, Wall: 0.94 s

Resultados de RSA
phi(n) =
420948928450589440622527756599631900264892349693029281297917230737847393\
694952758792056221851973205363997729970298101287180113772935641843325314\
```

```
0775276670269602560838144378160881763139984334160151123236538494767337 69\
8698202155023454321048413454212803191566763603235513572196668131604415 64\
3663707084394757607027256756986839638734238836874185601018010600839823 36
e =
1540434753343485114897016398822045759729660937306205268295043414080588 62\
0181523659966279509234163510674354320636735367093298730241129589411538 43\
1964127988884657635654889617824046060710843442734218998952222768080588 59\
9365481276447025837961800889882011405812000848733518014566347914596577 13\
1878572040283933708831715888404986586295424592071287886711674208679830 59
El mensaje cifrado es:
3803322228486889540590187935491476387433098127366599813979431363611940 39\
5060814754788669342859688815244225725187991430756578217807406535384925 04\
3435382279605174037471825701966938079343986815226766567047941408175734 04\
3986047275402710014809020233599504973966337740778552554932054823220753 70\
2997079747559769581600702377897997431379471406174299034328488934139014 21
Time: CPU 0.02 s, Wall: 0.03 s
```

Mensaje $m_5 = 6213292731514772349563846538563619013289101287432424124128272910601343094$

```
El mensaje original es:
6213292731514772349563846538563619013289101287432424124128272910601343 09\
4811187753654956266 7
p =
4738921664358131911202598545743618063192301104809939887375981394232371 78\
2861351961616243752487920165878407785672636681763286765213282725792997 56\
3378226436380268750642335646534018 53
q =
4504166492437201450839527442532666265291453347656372413283021672945024 45\
4091330279208029618439985297391897730070101996855293571151569612956991 75\
4084492348362100139859107940903343 87
n =
2134489217088663186922690716917660979081659536587052202856661329399726 61\
2975264594343172478477339921130991626234088499041984717134585420318320 18\
9083961950908602183579028740753698677560388634596673073138276781606879 47\
8199610360102524361350878330157957018684719774604079466908578412724729 25\
8095366806910391220624667498455275607015660283686929693800912058554191 11

Resultados del cifrado de Dickson
vn =
1898351757444905967446057773536992361493073204105460659791583429520401 51\
4255745553276215700510561881444658655945721991133377537470456083071065 07\
8758604023461099278813694888722465076527176843646827559676068621077048 81\
```

```
5076050613865405644500890740472908925508407797594278852014242662121254 67\
4648385196728841850662311978158042498835980205913952782209592925577387 80\
8527488477188724581625226339488362000622865808698078533798492710440669 73\
7238795021865953321701425330971632402384732011029321229788326184090829 20\
5558081020252832355406879786136189241164165453771621772284485469122635 48\
2300203446532939594566380571933502749423210464990303716183055246807008 26\
7529916910429838395567314313905434556395090372989100281106264270230456
k =
1668989842120354807249200720076014830898119531696285649162173574491600 04\
2009444938192444487443759348819602588086324698229465638546064398672825 65\
3662965313074162826386513830143917232865772918846649871410080803770849 17\
8790358388700738385900422638324583818326538630336517159725003301254040 97\
8835464488757755493250475058628899279072049757133592992401657883883063 90\
9907200806905704037014778567803028853762743816948870829070276869238584 22\
7972929420495612479817716162787928582625687429721913758128952411417231 84\
6066619632664570868542999664935763661027335374578856010220412308361019 73\
9234048581702042740279498626126848547603327768253488845216691727991720 06\
6318022524704639585741387471465004504776850010496087212878747406208 73
El mensaje cifrado con el sistema de cifrado de Dickson es c =
1873835490325048862874758590572844408704230131251173351319382552081506 67\
7970445078797357001243636610486812390808614349236923789566088948695933 81\
5662950569022410466260168666342269632419188779750031836126747645884401 45\
7139480107124994779854210467132366598569992558147596247545173133879973 55\
5882481098245688302955931691466179948290851263988929952310326643442060 24
Time: CPU 0.57 s, Wall: 1.04 s

Resultados de RSA
phi(n) =
2134489217088663186922690716917660979081659536587052202856661329399726 61\
2975264594343172478477339921130991626234088499041984717134585420318320 18\
9083961950908602183579028740753698668317300477801339711096150793330595 14\
9715855907636212060691875262980560781732037533779806095980672949454423 74\
2352628128291810884259815159705286289552941498944560803299468471116828 72
e =
4470384889711044953941444038671522125794733850644544156415421062865407 28\
3213428132182530374238175359263900786222759641597716889801769244434177 37\
0268035012018200100534945725370954288189465761238992741324639644327786 40\
8854124615603675546200937566623017777411960663359700438944662346107172 72\
8227662526100145336782046755006389044609604666321285223860915771466459 1
El mensaje cifrado es:
1522031694937054247622192653721533361004812142351716966656997997151070 56\
```

```
77734667593110547407963376698958471646287583030546643511200248933361690 3\
41934254690076877836129586992948405783690383398660137071827408515672953 9\
64445088596925426080584921739549562368727118003073175610686350968752450 5\
63429448664428324526138732319192452969790903196621669519945168788950092 7
Time: CPU 0.03 s, Wall: 0.05 s
```

4.4. Criptoanálisis

Ya que a diferencia del destinatario B un espía no conoce la factorización de n_B, éste no puede calcular la llave de descifrado t_B de la misma forma que lo hace B. Sin embargo podría tratar de utilizar otros métodos de descifrado, especialmente para hacer el descifrado parcial, esto es descifrar ciertos textos cifrados sin conocer la llave de descifrado t_B.

A continuación se discuten varios procedimientos de descifrado parcial, y en algunos casos se muestra que tales ataques pueden ser utilizados para factorizar n. Todos los ataques discutidos son análogos a los ataques conocidos contra el esquema RSA (cf. [25]). Para una discusión más algebraica de ataques de cifrado iterado sobre variantes del esquema RSA se puede consultar [21].

Nos restringimos al caso particular donde n es el producto de dos números primos impares distintos, es decir $n = p_1 p_2$. Se muestra que el esquema de cifrado de Dickson está a salvo de los ataques descritos en [19], si para $i = 1, 2$ el número p_i satisface lo siguiente[1]:

$$\begin{cases} p_i - 1 = a_i p_i^{'}, & \text{con } a_i < 10^5 \text{ y } p_i^{'} \text{ primo mayor a } 10^{80} \\ p_i + 1 = b_i p_i^{*}, & \text{con } b_i < 10^5 \text{ y } p_i^{*} \text{ primo mayor a } 10^{80} \end{cases} \tag{4.6}$$

y

$$\begin{cases} o_{p_i^{'}}(k) > 10^{11} \\ o_{p_i^{*}}(k) > 10^{11} \end{cases} \tag{4.7}$$

4.4.1. Ataques para encontrar un s con $D_s(c) \equiv 2 \pmod{n}$

Descifrado parcial

Sea $c \in \mathbb{Z}_n$ un texto cifrado dado. Supóngase que el criptoanalista tiene éxito en la búsqueda de un número natural s con $D_s(c) \equiv 2 \pmod{n}$. Sea $s = s_1 s_2$, donde cada factor primo de s_2 es primo relativo con k y el resto de los factores de s están en s_1 . Los números s_1 y s_2 pueden calcularse sin conocer la factorización de s, usando el siguiente algoritmo:

[1] $o_{p_i^{'}}(k)$ y $o_{p_i^{*}}(k)$ es el orden de k módulo $p_i^{'}$ y p_i^{*}, respectivamente.

Algoritmo 3.

Entrada: k, s
Salida: s_1, s_2
1. $s_1 \leftarrow 1$
2. $s_2 \leftarrow s$
3. Mientras $(s_2, k) > 1$
   3.1 $s_1 \leftarrow s_1(s_2, k)$
   3.2 $s_2 \leftarrow \frac{s_2}{(s_2,k)}$

El algoritmo 3 puede programarse en Mathematica como se muestra a continuación:

```
algoritmo3[k_, s_] := Module[{s1, s2},
  s1 = 1;
  s2 = s;
  mcd = GCD[s2, k];
  While[mcd > 1,
   s1 = s1*mcd;
   s2 = s2/mcd;
   mcd = GCD[s2, k];
    ];
  s1
  ]
```

Sean $u_i \in \mathbb{F}_{p_i^2}$, $i = 1, 2$ las soluciones de $u + \frac{1}{u} = c$. Tales soluciones siempre existen pues la ecuación es equivalente a $u^2 - uc + 1 = 0$. Como $D_s(c) \equiv 2 \pmod{n}$, entonces $D_s(c) \equiv 2 \pmod{p_i}$ con $i = 1, 2$. Usando (2.24) en $\mathbb{F}_{p_i^2}$ se satisface la ecuación

$$D_s(c) = D_s\left(u_i + \frac{1}{u_i}\right) = u_i^s + \frac{1}{u_i^s} = 2$$

de donde $u_i^{s^2} - 2u_i^s + 1 = 0$, por lo que $(u_i^s - 1)^2 = 0$ en $\mathbb{Z}_{p_i}$ para $i = 1, 2$ y por el Teorema Chino del Residuo $u_i^s = 1$ en $\mathbb{Z}_n$, es decir $u_i^{s_1 s_2} = 1$.

Recordemos que para que $D_k(x)$ sea polinomio de permutación módulo n es necesario que $(k, p_i^2 - 1) = 1$, así $(s_1, p_i^2 - 1) = 1$. Sea $o_i = o(u_i)$ en $\mathbb{F}_{p_i^2}$, por lo que $o_i | (p_i^2 - 1)$ y se tiene

$$(s_1, o_i) = 1. \tag{4.8}$$

De $u_i^{s_1 s_2} = 1$ se concluye que $o_i | s_1 s_2$, y por (4.8) se concluye que $o_i | s_2$, así $u_i^{s_2} = 1$. Por la forma en que se obtiene s_2 con el algoritmo 3 se tiene $(k, s_2) = 1$, por lo tanto existe $\bar{k} \in \mathbb{N}$ tal que $k\bar{k} \equiv 1 \pmod{s_2}$, de donde $k\bar{k} = s_2 r + 1$ para algún $r \in \mathbb{Z}$.

Si $m = D_k^{-1}(c) \equiv D_t(c) \pmod{n}$ es el texto en claro correspondiente a c, entonces la ecuación

$$m = D_t(c) = D_t\left(u_i + \frac{1}{u_i}\right) = u_i^t + \frac{1}{u_i^t}$$

se mantiene en $\mathbb{F}_{p_i^2}$ para $i = 1, 2$.

Por lo tanto

$$\begin{aligned} D_{\bar{k}}(c) &= D_{\bar{k}}\left(D_k(m)\right) = D_{\bar{k}k}(m) = D_{\bar{k}k}\left(u_i^t + \frac{1}{u_i^t}\right) = u_i^{t\bar{k}k} + \frac{1}{u_i^{t\bar{k}k}} \\ &= u_i^{t(s_2 r+1)} + \frac{1}{u_i^{t(s_2 r+1)}} = \left(u_i^{s_2}\right)^{tr} u_i^t + \frac{1}{\left(u_i^{s_2}\right)^{tr} u_i^t} = u_i^t + \frac{1}{u_i^t} = m \end{aligned}$$

en $\mathbb{F}_{p_i^2}$. Por el Teorema Chino del Residuo $D_{\bar{k}}(c) \equiv m \pmod{n}$.

Se supone que la búsqueda de un s tal que $D_s(c) \equiv 2 \pmod{n}$ se realiza mediante prueba y error, y más concretamente probando todas las s entre 1 y 10^5, el ataque se puede resumir en el siguiente algoritmo:

Algoritmo 4.

Entrada: n, k, c
Salida: m
1. $s \leftarrow 1$
2. Mientras $s < 10^5$ y $D_s(c) \not\equiv 2 \pmod{n}$
   2.1 $s \leftarrow s + 1$
3. Si $D_s(c) \not\equiv 2 \pmod{n}$
   3.1 **Salida**: "algoritmo sin éxito".
   3.2 Termina el algoritmo.
4. En otro caso
   4.1 Calcular s_1, s_2 con el algoritmo 3.
   4.2 $\bar{k} \leftarrow k^{-1} \mod s_2$
   4.3 $m \leftarrow D_{\bar{k}}(c) \mod n$

Una implementación en Mathematica queda de la siguiente manera:

```
(*ALGORITMO DE DESCIFRADO PARCIAL*)
descifradoparcial[n_, k_, c_] := Module[{s, s1, s2, k1, m},
  s = 1;
  While[s < 10^5 &&  dicksonpol[n, s, c] != 2,
    s = s + 1
   ];
  If[dicksonpol[n, s, c] != 2,
   Print["algoritmo sin éxito"],
   s1 = algoritmo3[k, s];
   s2 = s/s1;
   k1 = PowerMod[k, -1, s2];
   m = dicksonpol[n, k1, c];
   Print["s = ", s, "\n Mensaje orginal es ", m]
```

```
  ];
]
```

Ahora se mostrará que el cifrado de Dickson es seguro ante el ataque de descifrado parcial. Si se satisface (4.6) para $i = 1, 2$ se consideran las ecuaciones:

$$z + \frac{1}{z} = q, \text{ para alguna } q \in \mathbb{F}_{p_i}. \tag{4.9}$$

ó equivalentemente las ecuaciones cuadráticas $z^2 - qz + 1 = 0$.

Para $q = 2$ se tiene la ecuación $z^2 - 2z + 1 = 0$, la cual tiene una solución $z = 1$ de multiplicidad 2. Y si $q = -2$ la ecuación que hay que resolver es $z^2 + 2z + 1 = 0$ cuya solución es $z = -1$, también de multiplicidad 2.

Así que supondremos en lo que sigue que $q \neq \pm 2$.

Sean $M_i = \{u \in \mathbb{F}_{p_i^2} : u^2 - qu + 1 = 0\}$, $K_i = \{u \in \mathbb{F}_{p_i^2} : u^{p_i - 1} = 1\}$ y $L_i = \{u \in \mathbb{F}_{p_i^2} : u^{p_i+1} = 1\}$ para $i = 1, 2$.

Proposición 4.2. *Sean* $M = \{u \in \mathbb{F}_{p^2} : u^2 - qu + 1 = 0\}$, $K = \{u \in \mathbb{F}_{p^2} : u^{p-1} = 1\}$ *y* $L = \{u \in \mathbb{F}_{p^2} : u^{p+1} = 1\}$, *entonces* $M = K \cup L$.

Demostración. Sean $q \in \mathbb{F}_p$ y $0 \neq u \in \mathbb{F}_{p^2}$ tal que u es solución de la ecuación (4.9). Se demuestra que u^p es solución de (4.9) si y sólo si $u^p = u$ ó $u^p = u^{-1}$.

Supóngase primero que u^p es solución de (4.9), entonces $u^p + \frac{1}{u^p} = u + \frac{1}{u}$ la cual es equivalente a

$$(u^p - u)\left(1 - \frac{1}{u^{p+1}}\right) = 0 \tag{4.10}$$

de donde $u^p - u = 0$ ó $1 - \frac{1}{u^{p+1}} = 0$, por lo tanto $u^p = u$ ó $u^p = u^{-1}$.

Si se supone que $u^p = u$ ó $u^p = u^{-1}$, entonces u^p es solución de (4.9) pues sus soluciones son u y u^{-1}.

Con esto se tiene que $M = K \cup L$, como se deseaba.

□

Proposición 4.3. *Sean* $i = 1, 2$. *Entonces* K_i *y* L_i *son subgrupos de* $\mathbb{F}_{p_i^2}$.

Demostración. Notemos que $1 \in K_i$ pues $1^{p_i-1} = 1$. Sean $a, b \in K_i$, entonces $a^{p_i-1} = 1$ y $b^{p_i-1} = 1$ por lo que

$$(ab)^{p_i-1} = a^{p_i-1}b^{p_i-1} = 1$$

así $ab \in K_i$. Además $(a^{-1})^{p_i-1} = (a^{p_i-1})^{-1} = 1$, de este modo $a^{-1} \in K_i$. Por lo tanto K_i es subgrupo de $\mathbb{F}_{p_i^2}$.

Como $1^{p_i+1} = 1$, entonces $1 \in L_i$ y si $a, b \in L_i$ por la definición de L_i se cumple $a^{p_i+1} = 1$ y $b^{p_i+1} = 1$ así

$$(ab)^{p_i+1} = a^{p_i+1}b^{p_i+1} = 1$$

por lo tanto $ab \in L_i$, y también se cumple $(a^{-1})^{p_i+1} = (a^{p_i+1})^{-1} = 1$, luego $a^{-1} \in L_i$, de esta manera L_i es un subgrupo de $\mathbb{F}_{p_i^2}$. □

Proposición 4.4. *Si w es un generador del grupo $\mathbb{F}^*_{p_i^2}$ entonces $K_i = \langle w^{p_i+1}\rangle$ y $L_i = \langle w^{p_i-1}\rangle$. Además $|K_i| = p_i - 1$ y $|L_i| = p_i + 1$.*

Demostración. Considerando que $o(w) = p_i^2 - 1$.

Sea $u \in \langle w^{p_i+1}\rangle$, entonces u es de la forma $(w^{p_i+1})^r$ para alguna $r \in \mathbb{N}$. Al elevar u a la potencia $p_i - 1$ se obtiene $(w^{p_i+1})^{r(p_i-1)} = w^{(p_i^2-1)r} = 1$ por lo que $u \in K_i$, de este modo $\langle w^{p_i+1}\rangle \subseteq K_i$. Ahora sea $u \in K_i$, entonces $u \in \mathbb{F}^*_{p_i^2}$ por lo que $u = w^k$ para alguna $k \in \mathbb{N}$ y además $u^{p_i-1} = 1$ de donde $w^{(p_i-1)k} = 1$, pero $o(w) = p_i^2 - 1$ así que $(p_i - 1)(p_i + 1)|(p_i - 1)k$, es decir $(p_i + 1)|k$ luego $k = (p_i + 1)r$ con $r \in \mathbb{Z}$, en consecuencia $u = w^{(p_i+1)r} \in \langle w^{p_i+1}\rangle$, así que $K_i \subseteq \langle w^{p_i+1}\rangle$. Por lo tanto $K_i = \langle w^{p_i+1}\rangle$. Como $o(w) = p_i^2 - 1$, entonces $|\langle w^{p_i+1}\rangle| = p_i - 1$ y así $|K_i| = p_i - 1$.

Supóngase que $u \in \langle w^{p_i-1}\rangle$, entonces existe $r \in \mathbb{N}$ tal que $u = (w^{p_i-1})^r$. De esta manera $u^{p_i+1} = (w^{p_i-1})^{r(p_i+1)} = w^{(p_i^2-1)r} = 1$ así que $u \in L_i$, por lo tanto $\langle w^{p_i-1}\rangle \subseteq L_i$. Considerando $u \in L_i$ se tiene $u \in \mathbb{F}^*_{p_i^2}$ por lo que $u = w^k$ para alguna $k \in \mathbb{N}$ y como $u^{p_i+1} = 1$ se satisface $w^{(p_i+1)k} = 1$, de manera similar al párrafo anterior se tiene $(p_i - 1)|k$ de donde $k = (p_i - 1)r$ con $r \in \mathbb{Z}$, por lo que $u = w^{(p_i-1)r} \in \langle w^{p_i-1}\rangle$, así que $L_i \subseteq \langle w^{p_i-1}\rangle$. De esta manera $L_i = \langle w^{p_i-1}\rangle$ y como $o(w) = p_i^2 - 1$, entonces $|\langle w^{p_i-1}\rangle| = p_i + 1$ y así $|L_i| = p_i + 1$, como se deseaba.

□

Por la ecuación (4.6), $|K_i| = p_i - 1 = a_i p_i^{'}$ y $|L_i| = p_i + 1 = b_i p_i^*$.

Proposición 4.5. *Para $i = 1, 2$ si $u \in K_i$, entonces $o(u) \leq 10^5$ si y sólo si $o(u)|a_i$.*

Demostración. Sea $u \in K_i$, supóngase primero que $o(u)|a_i$, entonces $a_i = o(u)t$ para algún $t \in \mathbb{Z}$ y por (4.6) $a_i < 10^5$ de ahí que $o(u) \leq 10^5$.

Recíprocamente si $o(u) \leq 10^5$, como $u \in K_i$, entonces $u^{p_i-1} = 1$ y así $o(u)|(p_i - 1)$ pero $p_i - 1 = a_i p_i^{'}$ por lo que $o(u)|a_i p_i^{'}$, se tienen que $(o(u), p_i^{'})$ puede ser 1 o $d > 1$. Si $(o(u), p_i^{'}) = d > 1$ por ser $p_i^{'}$ primo se tendría $(o(u), p_i^{'}) = p_i^{'}$ de donde $o(u) = p_i^{'}t$ para algún $t \in \mathbb{Z}$ por (4.6) se tiene $p_i^{'} > 10^{80}$ y por lo tanto $o(u) > 10^{80}$ lo que es una contradicción, en consecuencia $(o(u), p_i^{'}) = 1$ y de este modo $o(u)|a_i$. □

Si $d|a_i$, entonces el número de elementos $u \in K_i$ con $o_{K_i}(u) = d$ está dado por $\varphi(d)$ (cf. [12]), y por lo tanto el número de elementos $u \in K_i$ con $o(u) \leq 10^5$ es $\sum_{d|a_i} \varphi(d) = a_i$.

Así se tiene:

$$\left|\left\{u \in K_i : o_{K_i}(u) \leq 10^5\right\}\right| = a_i \tag{4.11}$$

y de manera similar

$$\left|\left\{u \in L_i : o_{L_i}(u) \leq 10^5\right\}\right| = b_i \tag{4.12}$$

Para un texto cifrado $c \in \mathbb{Z}_n$, el algoritmo 4 es exitoso si y sólo si existe un s con $1 \leq s \leq 10^5$ tal que $D_s(c) \equiv 2 \pmod{n}$ ó equivalentemente, tal que s satisface $D_s(c) \equiv 2 \pmod{p_i}$ para $i = 1, 2$.

Si $u \in K_i \cup L_i$ es una solución de $u + \frac{1}{u} = c$, entonces $D_s(c) \equiv 2 \pmod{p_i}$ si y sólo si $u^s + \frac{1}{u^s} = 2$, lo que equivale a $u^s = 1$. Usando Teorema Chino del Residuo, (4.11) y (4.12) se obtiene que la cardinalidad del conjunto

$$\left\{c \in \mathbb{Z}_n : \exists s \text{ con } 1 \leq s \leq 10^5 \text{ tal que } D_s(c) \equiv 2 \pmod{n}\right\}$$

es menor ó igual a

$$\begin{aligned}
&\prod_{i=1}^{2} \left|\left\{c \in \mathbb{Z}_{p_i} : \exists s \text{ con } 1 \leq s \leq 10^5 \text{ tal que } D_s(c) \equiv 2 \pmod{p_i}\right\}\right| \\
&= \prod_{i=1}^{2} \left[\frac{1}{2}\left|\left\{u \in K_i \backslash \{\pm 1\} : o_{K_i}(u) \leq 10^5\right\}\right| + \frac{1}{2}\left|\left\{u \in L_i \backslash \{\pm 1\} : o_{L_i}(u) \leq 10^5\right\}\right| + 2\right] \\
&= \prod_{i=1}^{2} \left[\frac{1}{2}(a_i - 2) + \frac{1}{2}(b_i - 2) + 2\right] = \prod_{i=1}^{2} \left[\frac{1}{2}(a_i + b_i)\right] = \frac{1}{4}\prod_{i=1}^{2}(a_i + b_i) \\
&\leq \frac{1}{4}(10^5 \cdot 10^5) < 10^{10}.
\end{aligned}$$

Por lo tanto si (4.6) se cumple y si c está distribuido uniformemente sobre $\mathbb{Z}_n$, $n = p_1 p_2$ donde p_1 y p_2 son mayores que 10^{80}, entonces $n > 10^{160}$. De este modo la probabilidad de que c pueda ser descifrado por el algoritmo 4 es:

$$\frac{\left|\left\{c \in \mathbb{Z}_n : \exists s \text{ con } 1 \leq s \leq 10^5 \text{ tal que } D_s(c) \equiv 2 \pmod{n}\right\}\right|}{|\mathbb{Z}_n|} < \frac{10^{10}}{10^{160}} = 10^{-150},$$

es decir es prácticamente improbable.

Para ilustrar los ataques al sistema de cifrado de Dickson, se eligen números n con la condición de que sus factores primos fueron pequeños, en particular menores a 10^5.

Los ejemplos que se dan a continuación por cuestiones de tiempo de ejecución, fueron hechos con SAGE de acuerdo a los algoritmos que aparecen en el apéndice D.

Ejemplo 8. Sean $p_1 = 167$ y $p_2 = 859$, por lo que $n = 143453$, se eligió $k = 795565973$ y el mensaje a cifrar es $m = 436$.

El mensaje cifrado utilizando el sistema de cifrado basado en polinomios de Dickson y usando el algoritmo 2 es $c = 140269$.

Por lo que aplicando el descifrado parcial con SAGE se obtiene:

```
sage: descifradoparcial(143453,795565973,140269)
El mensaje original es m= 436
```

Ejemplo 9. Sean $p_1 = 1229$ y $p_2 = 9551$, por lo que $n = 11738179$, se elige como llave de cifrado $k = 976782073727$ y el mensaje a cifrar es $m = 237$.

El mensaje cifrado utilizando el sistema de cifrado basado en polinomios de Dickson y usando el algoritmo 2 es $c = 1071641$.

Por lo que aplicando el descifrado parcial con SAGE se obtiene:

```
sage: descifradoparcial(11738179,976782073727,1071641)
D_ 100000 ( 1071641 )mod 11738179  =  3200073
Algoritmo sin exito
```

Factorizando n

En ciertos casos, conociendo un s tal que $D_s(c) \equiv 2 \pmod{n}$ no sólo es posible descifrar c, también se puede factorizar n.

Para las siguientes consideraciones sea

$$v_2(s) = \text{máx}\{e \in \mathbb{N} : 2^e | s\}$$

Supóngase que por algún medio un criptoanalista ha encontrado una $s \in \mathbb{Z}$ par tal que $D_s(c) \equiv 2 \pmod{n}$. Sea $u_i \in \mathbb{F}_{p_i^2}$ para $i = 1, 2$, una solución de $u_i + u_i^{-1} = c$, de forma que $u_i^s = 1$. Se considera

$$\begin{aligned} j &= \text{máx}\{r \in [0, v_2(s)] : u_i^{s/2^r} = 1 \text{ con } i = 1, 2\} \\ &= \text{máx}\{r \in [0, v_2(s)] : D_{s/2^r}(c) \equiv 2 \pmod{n}\} \end{aligned}$$

Como la ecuación $x^2 = 1$ tiene exactamente 2 soluciones 1 y -1 en el grupo cíclico $\mathbb{F}_{p_i^2}^*$, $i = 1, 2$ se cumple uno de los siguientes cuatro casos:

1. $j = v_2(s)$.
2. $j < v_2(s)$, $u_1^{s/2^{j+1}} = 1$, $u_2^{s/2^{j+1}} = -1$.
3. $j < v_2(s)$, $u_1^{s/2^{j+1}} = -1$, $u_2^{s/2^{j+1}} = 1$.
4. $j < v_2(s)$, $u_1^{s/2^{j+1}} = -1$, $u_2^{s/2^{j+1}} = -1$.

El caso (1.) es equivalente a la congruencia $D_{s/2^{v_2(s)}}(c) \equiv 2 \pmod{n}$ y al caso (4.) le corresponde la siguiente identidad $D_{s/2^{j+1}}(c) \equiv -2 \pmod{n}$ pues para $i = 1, 2$ se satisface $u_i^{s/2^{j+1}} = -1$ por lo que $u_i^{s/2^{j+1}} + \frac{1}{u_i^{s/2^{j+1}}} = -1 - 1 = -2$ de este modo $D_{s/2^{j+1}}(c) \equiv -2 \pmod{p_i}$ y por el Teorema Chino del Residuo se sigue que $D_{s/2^{j+1}}(c) \equiv -2 \pmod{n}$.

Estos casos no dan información para factorizar n. En cambio, si el caso (2.) se cumple, entonces $D_{s/2^{j+1}}(c) \equiv 2 \pmod{p_1}$ y $D_{s/2^{j+1}}(c) \not\equiv 2 \pmod{p_2}$, y por lo tanto $\left(D_{s/2^{j+1}}(c) - 2, n\right) = p_1$, similarmente en el caso (3.) $D_{s/2^{j+1}}(c) \not\equiv 2 \pmod{p_1}$ y $D_{s/2^{j+1}}(c) \equiv 2 \pmod{p_2}$ de donde $\left(D_{s/2^{j+1}}(c) - 2, n\right) = p_2$, así se obtiene la factorización de n.

Si se asume que la búsqueda de s tal que $D_s(c) \equiv 2 \pmod{n}$ se hace probando todas las s pares entre 1 y 10^5, el ataque se resume en el siguiente algoritmo:

Algoritmo 5.

Entrada: n, c
Salida: d
1. $s \leftarrow 2$
2. Mientras $s < 10^5$ y $D_s(c) \not\equiv 2 \pmod{n}$
    2.1 $s \leftarrow s + 2$
3. Si $D_s(c) \not\equiv 2 \pmod{n}$
    3.1 **Salida**: "algoritmo sin éxito".
    3.2 Termina el algoritmo.
4. Calcular $v_2(s)$.
5. Calcular $j = \max\{r \in [0, v_2(s)] : D_{s/2^r}(c) \equiv 2 \pmod{n}\}$
6. Si $j = v_2(s)$
    6.1 **Salida**: "algoritmo sin éxito".
    6.2 Termina el algoritmo.
7. En otro caso
    7.1 Si $D_{s/2^{j+1}}(c) \equiv -2 \pmod{n}$
        7.1.1 **Salida**: "algoritmo sin éxito".
        7.1.2 Termina el algoritmo.
    7.2 En otro caso
        7.2.1 $d = \left(D_{s/2^{j+1}}(c) - 2, n\right)$

El programa para calcular $v_2(s)$ escrito en Mathematica, es:

```
V2[s_] := Module[{m, e},
  e = 1;
  While[Mod[s, 2^e] == 0,
   e = e + 1];
  m = e - 1;
  m
  ]
```

Para calcular el valor de j se utilizó el siguiente programa:

```
JMAX[c_, n_, s_, v2_] := Module[{r, max},
  For[r = 0, r <= v2,
   If[dicksonpol[n, s/2^r, c] == 2,
    max = r];
   r++];
  max
  ]
```

Así el algoritmo 5 implementado en Mathematica es:

```
(*ALGORITMO PARA FACTORIZAR n*)
factorizacion[n_, c_] := Module[{s, dic, v2, j, d},
  s = 2;
  While[s < 10^5 &&  dicksonpol[n, s, c] != 2,
    s = s + 2
   ];
  If[dicksonpol[n, s, c] != 2,
   Print["algoritmo sin éxito"];
   ];
  v2 = V2[s];
  j = JMAX[c, n, s, v2];
  If[j == v2,
   Print["Algoritmo sin éxito"],
   dic = dicksonpol[n, s/2^(j + 1), c];
   If[dic == -2,
    Print["Algoritmo sin éxito"],
    d = GCD[dic - 2, n];
    Print[n, " = ", d, " * ", n/d];
    ]]
  ]
```

Como el algoritmo 5 es exitoso sólo cuando el texto cifrado c puede ser descifrado con el algoritmo 4, aquel algoritmo no representa una amenaza real para el cifrado de Dickson. Si la condición (4.6) se cumple y si c está distribuido uniformemente sobre $\mathbb{Z}_n$, entonces la probabilidad de que el algoritmo 5 dé como resultado un factor no trivial de n es menor a 10^{-150}.

Los siguientes ejemplos fueron hechos con SAGE, como lo muestran los algoritmos del apéndice D, ya que los hechos en Mathematica son mucho más lentos y su capacidad para realizar los cálculos es limitada.

Ejemplo 10. Sean $p_1 = 443$ y $p_2 = 83$, por lo que $n = 36769$, se eligió $k = 34233781$ y el mensaje a cifrar es $m = 91$.

El mensaje cifrado utilizando el sistema de cifrado basado en polinomios de Dickson y usando el algoritmo 2 es $c = 28477$.

Por lo que aplicando el ataque para factorizar n con SAGE se obtiene:

```
sage: factorizacion(36769,28477)
36769  =  83  *  443
```

Ejemplo 11. Sean $p_1 = 137$ y $p_2 = 523$, por lo que $n = 71651$, se eligió $k = 198331723$ y el mensaje a cifrar es $m = 785$.

El mensaje cifrado utilizando el sistema de cifrado basado en polinomios de Dickson y usando el algoritmo 2 es $c = 33449$.

Por lo que aplicando el descifrado parcial con SAGE se obtiene:

```
sage: factorizacion(71651,33449)
Algoritmo sin exito
```

4.4.2. Factorizando por medio de puntos fijos

Sea $n = p_1p_2$ con p_i primo impar, $i = 1{,}2$ y sea s un número natural impar, y sea $c \in \mathbb{Z}_n$ tal que $c \not\equiv \pm 2 \pmod{n}$ es un punto fijo de $D_s(x) \mod n$, es decir $D_s(c) \equiv c \pmod{n}$. Claramente c también satisface que es un punto fijo de $D_s(x) \mod p_i$ para $i = 1, 2$. Sea $u_i \in GF(p_i^2)$ una solución de $u_i + \frac{1}{u_i} = c$, $i = 1, 2$. Entonces se tiene

$$D_s(c) = D_s\left(u_i + \frac{1}{u_i}\right) = u_i^s + \frac{1}{u_i^s} = u_i + \frac{1}{u_i}$$

por lo tanto $\frac{u_i^{2s}+1}{u_i^s} = \frac{u_i^2+1}{u_i}$, lo que es equivalente a:

$$\begin{aligned} -u_i^{s+1} - u_i^{s-1} + u_i^{s+1+s-1} + 1 &= 0 \\ u_i^{s+1}(u_i^{s-1} - 1) - (u_i^{s-1} - 1) &= 0 \\ (u_i^{s-1} - 1)(u_i^{s+1} - 1) &= 0 \end{aligned}$$

de donde $u_i^{s+1} = 1$ ó $u_i^{s-1} = 1$.

Además por ser $c = u_i + \frac{1}{u_i}$, $D_{s+1}(c) = u_i^{s+1} + \frac{1}{u_i^{s+1}} \equiv 2 \pmod{p_i}$ si y sólo si $u_i^{s+1} = 1$. De manera similar $u_i^{s-1} = 1$ es equivalente a $D_{s-1}(c) \equiv 2 \pmod{p_i}$.

Si $u_1^{s+1} = 1$ y $u_2^{s-1} = 1$, pero no $u_2^{s+1} = 1$, o bien $u_1^{s-1} = 1$ y $u_2^{s+1} = 1$, pero no $u_2^{s-1} = 1$, entonces $(D_{s+1}(c) - 2, n) \in \{p_1, p_2\}$, y así se ha encontrado un factor de n.

Sin embargo, si $u_1^{s+1} = 1$ y $u_2^{s+1} = 1$, ó $u_1^{s-1} = 1$ y $u_2^{s-1} = 1$, entonces se ha encontrado un número $\bar{s}$ impar con $D_{\bar{s}}(c) \equiv 2 \pmod{n}$ y por lo tanto se puede aplicar el ataque anterior.

Un caso especial de este ataque se da, cuando $s = k$. Entonces c es un punto fijo del polinomio de cifrado $D_k(x) \mod n$. Como no se conoce algún algoritmo para la búsqueda de puntos fijos de $D_s(x) \mod n$, sólo se usan métodos de prueba y error. Por lo tanto el cifrado de Dickson es seguro ante este ataque, si el número $fij(n, x)$ de puntos fijos de $D_s(x) \mod n$ es pequeño. Por el Teorema Chino del Residuo $fij(n, s) = \prod_{i=1}^{2} fij(p_i, s)$ y por el teorema C.1 del apéndice de puntos fijos se tiene

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

Si los parámetros de la llave satisfacen (4.6), entonces

$$\begin{aligned} fij(p_i, s) &= \frac{1}{2}\left[(s-1, a_i)(s-1, p_i^{'}) + (s+1, a_i)(s+1, p_i^{'})\right] \\ &\quad + \frac{1}{2}\left[(s-1, b_i)(s-1, p_i^{*}) + (s+1, b_i)(s+1, p_i^{*})\right] - 2 \end{aligned}$$

Si para $i = 1, 2$

$$p_i^{'} \nmid (s-1),\ p_i^{'} \nmid (s+1),\ p_i^{*} \nmid (s-1), p_i^{*} \nmid (s+1) \tag{4.13}$$

se satisface $(p_i^{'}, s-1) = (p_i^{'}, s+1) = (p_i^{*}, s-1) = (p_i^{*}, s+1) = 1$ así que

$$fij(p_i, s) = \frac{1}{2}\left[(s-1, a_i) + (s+1, a_i) + (s-1, b_i) + (s+1, b_i)\right] - 2 \leq 2 \cdot 10^5 < 10^6$$

y en consecuencia $fij(n, s) < 10^{12}$. En este caso la probabilidad de que un $c \in \mathbb{Z}_n$, distribuido uniformemente en $\mathbb{Z}_n$, sea un punto fijo de $D_s(x)$ mód n es menor a $10^{12}/10^{160} = 10^{-148}$, así la tarea de encontrar un punto fijo no es factible computacionalmente.

Supóngase que el número s es elegido de acuerdo a una distribución uniforme en $M = \{1, 2, \ldots, r\}$, donde r es un entero positivo grande, por ejemplo $r = 10^{100}$. Consideremos $\lfloor x \rfloor$ como la función máximo entero menor ó igual que x. Con esta notación hay exactamente $\left\lfloor \frac{r-1}{p_i^{'}} \right\rfloor + 1$ números $s \in M$ tales que $p_i^{'} | (s-1)$. Sean $1, 1+p_i^{'}, 1+2p_i^{'}, \ldots, 1+\left\lfloor \frac{r-1}{p_i^{'}} \right\rfloor$ tales números. De manera similar hay exactamente $\left\lfloor \frac{r-1}{p_i^{*}} \right\rfloor + 1$ números $s \in M$ tales que $p_i^{*} | (s-1)$, $\left\lfloor \frac{r+1}{p_i^{'}} \right\rfloor$ números $s \in M$ tales que $p_i^{'} | (s+1)$ y existen $\left\lfloor \frac{r+1}{p_i^{*}} \right\rfloor$ números $s \in M$ tales que $p_i^{*} | (s+1)$. Es decir:

$$\begin{aligned} |\{s \in M : p_i^{'} | (s-1)\}| &= \left\lfloor \frac{r-1}{p_i^{'}} \right\rfloor + 1 \\ |\{s \in M : p_i^{*} | (s-1)\}| &= \left\lfloor \frac{r-1}{p_i^{*}} \right\rfloor + 1 \\ |\{s \in M : p_i^{'} | (s+1)\}| &= \left\lfloor \frac{r+1}{p_i^{'}} \right\rfloor \\ |\{s \in M : p_i^{*} | (s+1)\}| &= \left\lfloor \frac{r+1}{p_i^{'}} \right\rfloor \end{aligned}$$

Como $p_i^{'} > 10^{80}$, se obtiene:

$$\left\lfloor \frac{r-1}{p_i^{'}} \right\rfloor + 1 \leq \left\lfloor \frac{r}{p_i^{'}} \right\rfloor + 1 \leq \left\lfloor \frac{r}{10^{80}} \right\rfloor + 1$$

también

$$\left\lfloor \frac{r+1}{p_i'} \right\rfloor \leq \left\lfloor \frac{r}{p_i'} \right\rfloor + 1 \leq \left\lfloor \frac{r}{10^{80}} \right\rfloor + 1.$$

De la misma manera por ser $p_i^* > 10^{80}$ se satisface

$$\left\lfloor \frac{r-1}{p_i^*} \right\rfloor + 1 \leq \left\lfloor \frac{r}{p_i^*} \right\rfloor + 1 \leq \left\lfloor \frac{r}{10^{80}} \right\rfloor + 1$$

y

$$\left\lfloor \frac{r+1}{p_i^*} \right\rfloor \leq \left\lfloor \frac{r}{p_i^*} \right\rfloor + 1 \leq \left\lfloor \frac{r}{10^{80}} \right\rfloor + 1.$$

Por lo tanto

$$|\{s \in M : p_i'|(s-1) \text{ ó } p_i'|(s+1) \text{ ó } p_i^*|(s-1) \text{ ó } p_i^*|(s+1)\}| \leq 4\left(\left\lfloor \frac{r}{10^{80}} \right\rfloor + 1\right).$$

En consecuencia, un límite inferior para la probabilidad de que un $s \in M$ distribuido uniformemente satisfaga (4.13), está dado por

$$\frac{r - 4\left(\left\lfloor \frac{r}{10^{80}} \right\rfloor + 1\right)}{r} = \frac{r - \frac{4r}{10^{80}} - 4}{r} = 1 - \frac{4}{10^{80}} - \frac{4}{r}.$$

De este modo si los elementos de M están distribuidos uniformemente es casi seguro que cumpla (4.13).

Así, si los parámetros de la clave k y n satisfacen (4.6), entonces la tarea de encontrar $s \in \mathbb{N}$ y $c \in \mathbb{Z}_n$ tales que c sea un punto fijo de $D_s(x) \pmod n$ no es factible computacionalmente.

4.4.3. Cifrado iterado

Sea $c \in \mathbb{Z}_n$ un texto cifrado dado. Se consideran $D_k(c), D_k^2(c), D_k^3(c), \ldots$, donde $D_k^r(c)$ denota la función $D_k(x)$ iterada r veces. Como $\mathbb{Z}_n$ es finito, hay dos exponentes $r, s \in \mathbb{N}$ tales que $D_k^r(c) \equiv D_k^s(c) \pmod n$, esto implica la existencia de $t \in \mathbb{N}$ tal que $D_k^t(c) \equiv c \pmod n$, ó equivalentemente por la propiedad 2 del lema 2.2 es posible encontrar $t \in \mathbb{N}$ tal que $D_{k^t}(c) \equiv c \pmod n$.

Si m denota el texto en claro correspondiente a c, es decir $c \equiv D_k(m) \pmod n$, entonces:

$$\begin{aligned} D_k^{t+1}(m) &\equiv D_k^t\left(D_k(m)\right) \pmod n \equiv D_k^t(c) \pmod n \\ &\equiv c \pmod n \equiv D_k(m) \pmod n \end{aligned}$$

De esta manera $D_k^t(m) \equiv m \pmod n$ y por lo tanto:

$$\begin{aligned} D_k^{t-1}\left(D_k(m)\right) &\equiv m \pmod n \\ D_k^{t-1}(c) &\equiv m \pmod n \end{aligned}$$

con lo que se recupera el texto en claro.

A veces el cifrado iterado también da la factorización de n. Es decir, a partir de $D_k^t(c) \equiv c \pmod{n}$ se sigue $D_{k^t}(c) \equiv c \pmod{n}$, lo que significa que c es un punto fijo de $D_{k^t}(x) \mod n$, y como k^t es impar, puede utilizarse el ataque por medio de puntos fijos.

El ataque de cifrado iterado sólo tiene éxito si existe t pequeño, digamos $t \leq 10^{10}$, tal que c es un punto fijo de $D_{k^t}(x) \mod n$. Así el cifrado de Dickson es seguro ante este ataque, si para todo $t \leq 10^{10}$ la función $D_{k^t}(x) \mod n$ tiene sólo un número pequeño de puntos fijos.

Supóngase que se satisfacen las condiciones (4.6) y (4.7). Entonces todo t tal que $1 \leq t \leq 10^{10}$ cumple $k^t \not\equiv \pm 1 \pmod{p_i'}$ y $k^t \not\equiv \pm 1 \pmod{p_i^*}$, de donde

$$\begin{aligned}
fij(p_i, k^t) &= \frac{1}{2}\left[(k^t - 1, a_i p_i') + (k^t + 1, a_i p_i') + (k^t - 1, b_i p_i^*) + (k^t + 1, b_i p_i^*)\right] - 2 \\
fij(p_i, k^t) &= \frac{1}{2}\left[(k^t - 1, a_i)(k^t - 1, p_i') + (k^t + 1, a_i)(k^t + 1, p_i')\right] \\
&\quad + \frac{1}{2}\left[(k^t - 1, b_i)(k^t - 1, p_i^*) + (k^t + 1, b_i)(k^t + 1, p_i^*)\right] - 2 \\
&= \frac{1}{2}\left[(k^t - 1, a_i) + (k^t + 1, a_i) + (k^t - 1, b_i) + (k^t + 1, b_i)\right] - 2 \\
&\leq 2 \cdot 10^5 - 2 < 10^6
\end{aligned}$$

y por lo tanto $fij(n, k^t) < 10^{12}$.

Esto da lugar a que

$$\begin{aligned}
|\{c \in \mathbb{Z}_n : \exists t \in \mathbb{N} \text{ con } t \leq 10^{10} \text{ y } D_{k^t}(c) \equiv c \pmod{n}\}| &< \sum_{t=1}^{10^{10}} fij(n, k^t) \\
&< 10^{10} \cdot 10^{12} = 10^{22}.
\end{aligned}$$

Por lo tanto, si las condiciones (4.6) y (4.7) se satisfacen, entonces la fracción de textos cifrados $c \in \mathbb{Z}_n$ que pueden ser descifrados con el ataque de cifrado iterado está limitada por

$$\frac{|\{c \in \mathbb{Z}_n : \exists t \in \mathbb{N} \text{ con } t \leq 10^{10} \text{ y } D_{k^t}(c) \equiv c \pmod{n}\}|}{|\mathbb{Z}_n|} = \frac{10^{22}}{10^{160}} = 10^{-138}$$

.

Capítulo 5

Intercambio de claves

Los sistemas de cifrado clásicos basan su seguridad en mantener oculta la clave usada para cifrar datos. Los participantes en el intercambio de información no deben decir públicamente cuál es la clave que están empleando para establecer la comunicación, así que deben ponerse de acuerdo con anterioridad. En 1976 Whitfield Diffie y Martin Hellman publicaron un artículo titulado *New directions in cryptography* [8] en el que se expone un mecanismo mediante el cual es posible que dos personas pueden ponerse de acuerdo en una palabra clave secreta comunicándose a gritos entre una multitud que no debe conocer su secreto (es decir comunicándose mediante un canal inseguro) y que puede conocer el algoritmo utilizado.

En este capítulo presentamos el algoritmo de intercambio de claves de Diffie - Hellman que se basa en un problema muy importante en Teoría de Números que es el problema del logaritmo discreto (PLD). Análogamente al PLD se define el problema de Dickson discreto (PDD) y se analiza un algoritmo de intercambio de clave basado en polinomios de permutación de Dickson y PDD (cf. [28]).

5.1. El problema del logaritmo discreto

En está sección se recuerda el problema del logaritmo discreto que es muy útil en criptografía. Considere $(G, *)$ un grupo cíclico de orden n bajo la operación $*$, y defina para $\alpha \in G$ y $m \in \mathbb{N}$ $\alpha^m = \alpha * \alpha * \cdots * \alpha$, es decir α^m es el resultado de operar m veces α bajo $*$. Sea $\alpha \in G$ tal que $G = \langle \alpha \rangle$.

Definición 5. *Sea $\beta \in G$ distinto de la identidad, el* ***logaritmo discreto*** *de β en base α es el entero x tal que $1 \leq x < n$ y $\alpha^x = \beta$ en G.*

Ejemplo 12. *Sea $G = \mathbb{Z}_7^*$ el grupo multiplicativo de $\mathbb{Z}_7$, cuyo orden es 6 y un generador es 3. El logaritmo discreto de 4 en base 3 es 4 pues $3^4 \equiv 4$ (mód 7).*

El problema del logaritmo discreto (PLD) se considera computacionalmente imposible de resolver. Esto se debe a que hasta el momento no existe un algoritmo eficiente capaz de calcular el logaritmo discreto en un grupo arbitrario.

La seguridad de muchas técnicas de cifrado depende de la dificultad de resolver el PLD, entre ellas: intercambio de claves Diffie-Hellman y sus derivados, el cifrado de ElGamal, el esquema de firma ElGamal y sus variantes entre los que destacan los estándares DSA y firma con curvas elípticas (cf. [17]).

5.2. Intercambio de claves (Diffie-Hellman)

Se describe el primer modelo que permite a dos personas acordar el uso de una clave privada, utilizando un medio inseguro.

Sean Alicia y Beto (A y B respectivamente) dos participantes de una red de comunicación que desean obtener una clave secreta en común. El algoritmo de intercambio de claves de Diffie - Hellman es el siguiente:

1. Alicia y Beto se ponen de acuerdo en un par de números: un primo grande p y un generador $g \in \mathbb{Z}_p^*$. Se pueden poner de acuerdo públicamente en un canal inseguro.
2. Alicia elige un entero aleatorio α, con $0 < \alpha < p-1$, y le envía a Beto
$$X = g^\alpha \text{ mód } p.$$
3. Beto elige un entero aleatorio β, con $0 < \beta < p-1$, y le envía a Alicia
$$Y = g^\beta \text{ mód } p.$$
4. Alicia calcula $K = Y^\alpha$ mód p.
5. Beto calcula $K' = X^\beta$ mód p.

Se tiene que $K = K' = g^{\alpha\beta}$ módp. Nadie que haya estado escuchando la conversación entre Alicia y Beto puede calcular K. Un atacante sólo conocería p, g, X, Y, y para calcular K tendría que poder obtener α o β, es decir debería ser capaz de calcular un logaritmo discreto.

En [26] se describen algoritmos para realizar el punto 1.

5.3. El problema de polinomios de Dickson

En esta sección se describe un análogo al PLD utilizando polinomios de Dickson. Probaremos que la dificultad de resolver $b = D_n(x) \mod m$, es decir dados $m, b, x \in \mathbb{Z}$ encontrar $n \in \mathbb{Z}$ que satisfaga la igualdad $b = D_n(x) \mod m$, es equivalente a la dificultad de resolver el problema usual del logaritmo discreto, que se aplica en la práctica para el intercambio de claves.

Definición 6. *Sea R un anillo conmutativo con identidad. Dados y, u el problema de calcular el valor de $n \in \mathbb{N}$ tal que $y = D_n(u)$ es llamado el problema de Dickson discreto (PDD).*

Teorema 5.1. *Sea $\mathbb{F}_q$ un campo finito, entonces:*

1. *Para $y = D_n(u)$, PDD puede resolverse encontrando las soluciones de a lo más dos PLD sobre $\mathbb{F}_{q^4}$.*
2. *PLD es equivalente al PDD sobre el campo finito $\mathbb{F}_q$.*

Demostración. Se busca x tal que $u = x + x^{-1}$ esto es

$$x^2 - ux + 1 = 0, \tag{5.1}$$

tal x existe en $\mathbb{F}_{q^2}$.

Luego $y = D_n(u) = D_n(x + x^{-1}) = x^n + x^{-n}$ de ahí que

$$x^2 - ux + 1 = 0 \text{ y } x^{2n} - yx^n + 1 = 0 \tag{5.2}$$

esta ecuación cuadrática tiene solución x^n en $\mathbb{F}_{(q^2)^2}$.

Nótese que x^{-1} y x^{-n} son solución de (5.1) y (5.2), respectivamente.

Si e es una solución de (5.2), debe resolverse el PLD para $x^m = e$ donde x es una solución de (5.1). Entonces $m = n$ ó $m = -n$, pues se evalúa $D_m(u)$ y $D_{-m}(u)$, de donde se tendría $y = D_m(u)$ ó $y = D_{-m}(u)$.

Para la segunda parte supóngase que se quiere calcular el entero n tal que $a^n = b$ para $a \in \mathbb{F}_q^*$, y b un elemento del subgrupo generado por a. Sean x, y como sigue:

$$\begin{cases} x = a + a^{-1} \\ y = b + b^{-1} \end{cases} \tag{5.3}$$

Basándonos en la ecuación $D_n(u + u^{-1}) = u^n + u^{-n}$, se tiene que $y = D_n(x)$ es igual a $b + b^{-1} = a^n + a^{-n}$, que se puede reescribir como:

$$b - a^n = \frac{1}{a^n} - \frac{1}{b} = \frac{b - a^n}{ba^n} \tag{5.4}$$

es decir

$$\begin{aligned} (b - a^n)ba^n - b + a^n &= 0 \\ (b - a^n)ba^n - (b - a^n) &= 0 \\ (b - a^n)(ba^n - 1) &= 0 \end{aligned} \tag{5.5}$$

La ecuación (5.5) se cumple si y sólo si $a^n = b$ ó $ba^n = 1 = a^{q-1}$, en el segundo caso $b = a^{q-1}a^{-n} = a^{q-1-n}$.

Para los x, y dados, después de resolver el PDD se obtiene n' la cual satisface la ecuación (5.5), es decir, si $a^{n'} = b$ entonces $n = n'$, de otra manera $a^{q-1-n'} = b$ implica que $n = q - 1 - n'$, con esto se resuelve el PLD. Recíprocamente si se resuelve el PLD se obtendría n tal que $a^n = b$, y por la forma que se definieron x, y en (5.3) se tendría la solución al PDD, es decir se encuentra el valor de n tal que $y = D_n(x)$.

En los dos casos, el PLD es equivalente con el PDD cuando (5.4) se cumple. Esto completa la demostración. □

Teorema 5.2. *La dificultad de resolver el PDD es igual a la del PLD sobre un campo finito* $\mathbb{F}_q$.

Demostración. De acuerdo a (2.) del teorema (5.1), podemos deducir que la dificultad de resolver PDD es igual a la del PLD sobre un campo finito $\mathbb{F}_q$. □

5.4. Intercambio de claves basado en polinomios de Dickson

Basado en los polinomios de Dickson sobre un campo finito con 2^m elementos, se puede construir un nuevo protocolo de acuerdo de claves parecido al algoritmo de Diffie - Hellman.

A continuación se lista la notación usada para describir el algoritmo:

A cliente.

B servidor.

PW contraseña de A.

ID_A, ID_B números de identificación de A y B, respectivamente.

r_A, r_B enteros aleatorios elegidos por A y B, respectivamente. Estos elementos se pondrán en base 2 para verlos como elementos de $\mathbb{F}_{2^m}$, donde $m \geq 2$.

n_A, n_B enteros elegidos por A y B, respectivamente.

β número aleatorio y la clave privada del servidor.

$D_n(x)$ polinomio de Dickson en $\mathbb{F}_{2^m}$ de grado n, $m \geq 2$ y n impar tal que $n \not\equiv 0 \pmod 3$.

HASH Función hash pública libre de colisiones.

|| Operación de concatenación.

Un ejemplo de función hash libre de colisiones es SHA-3, que se describe brevemente en el apéndice B.

Supóngase que A y B comparten el valor de la función HASH:

$$h = \text{HASH}(ID_A||ID_B||\beta||PW).$$

El protocolo de acuerdo de claves funciona como sigue:

1. A elige un número aleatorio r_A y en entero n_A, calcula

   $$AU_1 = \text{HASH}(h||r_A||n_A||ID_A)$$

   y envía AU_1, r_A, n_A, ID_A a B.

2. B calcula $AU_1^{'} = \text{HASH}(h||r_A||n_A||ID_A)$, compara si $AU_1 = AU_1^{'}$, en caso de que no se satisfaga la igualdad, entonces B abandona el protocolo; en otro caso, A es autenticado y B va al siguiente paso.

3. B elige un número aleatorio r_B y en entero n_B, calcula

   $$AU_2 = \text{HASH}(h||r_B||n_B||ID_B)$$

   y envía AU_2, r_B, n_B, ID_B al cliente A.

4. A calcula $AU_2^{'} = \text{HASH}(h||r_B||n_B||ID_B)$, compara si $AU_2 = AU_2^{'}$, si se satisface la igualdad, entonces B es autenticado y A va al siguiente paso; en otro caso, A no sigue adelante con el protocolo.

5. A calcula $m = r_A r_B, x_0 = (r_A + r_B)$ donde $x_0 \in \mathbb{F}_{2^m}$, elige un entero impar P_A tal que $P_A \not\equiv 0 \pmod 3$ y calcula

   $$x = D_{P_A}(x_0),\ AU_3 = \text{HASH}(h||n_B)$$

   y envía x, AU_3 a B.

6. B calcula $m = r_A r_B, x_0 = (r_A + r_B)$ donde $x_0 \in \mathbb{F}_{2^m}$, elige un entero impar P_B tal que $P_B \not\equiv 0 \pmod 3$ y calcula

   $$y = D_{P_B}(x_0),\ AU_4 = \text{HASH}(h||n_A)$$

   y envía la pareja y, AU_4 al cliente A.

7. A calcula $AU_4^{'} = \text{HASH}(h||n_A)$ compara si $AU_4 = AU_4^{'}$, si la relación se cumple, A calcula la clave secreta como

   $$K = D_{P_A}(y) = D_{P_A}(D_{P_B}(x_0)),$$

   en caso contrario da por terminada su sesión con B.

8. B calcula $AU_3' = \text{HASH}(h||n_B)$ compara si $AU_3 = AU_3'$, si la relación se cumple, B calcula la clave secreta como

$$K' = D_{P_B}(x) = D_{P_B}(D_{P_A}(x_0)),$$

en otro caso considera que A falló al autenticarse y cierra su sesión con A.

El algoritmo es correcto pues ya se demostró que se satisface la igualdad $D_{P_A}(D_{P_B}(x_0)) = D_{P_B}(D_{P_A}(x_0))$, por lo que la clave de sesión se puede utilizar para la comunicación segura entre A y B.

5.4.1. Seguridad del algoritmo de intercambio de clave

Recuérdese que los polinomios de Dickson están relacionados con los polinomios de Chebyshev por la igualdad (1.5), y en [1] se muestra un ataque a un sistema de cifrado basado en polinomios de Chebyshev, el cual presentamos brevemente:

Sistema de cifrado basado en polinomios de Chebyshev

Un sistema de cifrado de llave pública basado en polinomios de Chebyshev fue propuesto en [10], y puede ser visto como una generalización del sistema de cifrado de llave pública ElGamal, el cual se describe en [17]. El sistema de cifrado basado en polinomios de Chebyshev es el siguiente:

Generación de llave
A realiza lo siguiente:

1. Genera un entero grande s.
2. Elige un número aleatorio $x \in [-1, 1]$ y calcula $T_s(x)$.
3. La clave pública de A es $(x, T_s(x))$ y su clave privada es s.

Cifrado
B realiza lo siguiente:

1. Obtiene la llave pública de autenticación de A, que es $(x, T_s(x))$.
2. Representa el mensaje como un número $M \in [-1, 1]$.
3. Genera un número grande r.
4. Calcula $T_r(x), T_{r\cdot s}(x) = T_r(T_s(x))$ y $X = M \cdot T_{r\cdot s}(x)$.
5. Envía el texto cifrado $C = (T_r(x), X)$ al usuario A.

Descifrado
A recobra del texto cifrado C, el texto en claro M, haciendo lo siguiente:

1. Usa su clave privada para calcular $T_{s\cdot r}(x) = T_s(T_r(x))$.
2. Recobra M calculando $M = \frac{X}{T_{s\cdot r}(x)}$.

Ataque de Bergamo
Bergamo propone en [1] el siguiente ataque para demostrar que el esquema es inseguro:

1. Se calcula r' tal que $T_{r'}(x) = T_r(x)$.
2. Se evalúa $T_{r'\cdot s}(x) = T_{r'}(T_s(x))$.
3. Recupera $M = \frac{X}{T_{r'\cdot s}(x)}$.

Por lo tanto el ataque de Bergamo está basado en la condición de que un adversario puede obtener los elementos $x, T_r(x)$ y $T_{r'}(x)$.

Notemos que en el protocolo de intercambio de claves basado en polinomios de Dickson, r_A y r_B son públicos por lo que un adversario puede calcular $m = r_A r_B$ y $x_0 = r_A + r_B \in \mathbb{F}_{2^m}$. Como en el paso 5 y 6 se tienen: $x = D_{P_A}(x_0)$, $y = D_{P_B}(x_0)$, además los valores x, y son públicos, el ataque de Bergamo adaptado a este protocolo de intercambio de claves es:

1. Se calcula r' tal que $D_{r'}(x_0) = y$.
2. Se evalúa $D_{r'}(x)$.
3. Obtiene la clave K, como $K = D_{r'}(x)$, es decir $K = D_{r'}(x) = D_{r'}(D_{P_A}(x_0))$.

De este modo para encontrar r' tal que $D_{r'}(x_0) = y$, se tiene que resolver el PDD, que actualmente es imposible en tiempo real como lo muestra el teorema 5.2, si m es suficientemente grande. Esto hace que el protocolo de intercambio de claves basado en polinomios de Dickson sea resistente al ataque de Bergamo.

Apéndice A

RSA

El RSA es un criptosistema de llave pública, fue desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman [23], de ahí el nombre de RSA, que corresponde a las iniciales de los apellidos de sus autores. Este criptosistema, fue el primero de clave pública y actualmente es uno de los más populares por su uso en internet.

Para crear las claves (pública y privada) en el RSA, primero se eligen dos números primos p, q diferentes y que sean lo suficientemente grandes, en la práctica se recomienda que sean del orden de 10^{200}, se calcula el producto $N = pq$. En seguida se evalúa la función de Euler $\varphi(N) = (p-1)(q-1)$, y se selecciona un número entero positivo e tal que $e \in \mathbb{Z}^*_{\varphi(N)}$. Por último se calcula la inversa de e módulo $\varphi(N)$, es decir se calcula d tal que $ed \equiv 1$ mód $\varphi(N)$.

De esta manera la clave pública es la pareja (N, e), mientras que la clave privada es d.

El conjunto de textos en claro y textos cifrados ambos corresponden a $\mathbb{Z}_N$. Así para cifrar un mensaje m se tiene que el texto cifrado corresponde a

$$c \equiv m^e \text{ mód } N. \tag{A.1}$$

Para descifrar c, se usa la clave privada d calculando

$$m \equiv c^d \text{ mód } N, \tag{A.2}$$

el cual corresponde al mensaje original.

El descifrado funciona pues si $(m, N) = 1$ y $c \equiv m^e$ mód N, entonces $c^d \equiv m^{ed}$ mód N y de acuerdo a como se consideran e y d se tiene que $ed \equiv 1$ mód $\varphi(N)$, de donde $ed = t\varphi(N) + 1$ para algún $t \in \mathbb{Z}$, así que usando el Teorema de Euler se tiene

$$c^d \equiv m^{ed} \text{ mód } N \equiv m^{t\varphi(N)} m \text{ mód } N \equiv m \text{ mód } N$$

Por otro lado, si $(m, N) > 1$, se descifra c con ayuda del Teorema Chino del Residuo de la siguiente forma:

- Calcular q', p', el inverso de q (mód p) y p (mód q), respectivamente.

- Calcular $s \equiv c^{d \pmod{p-1}} \pmod{p}$ y $t \equiv c^{d \pmod{q-1}} \pmod{q}$.
- Recuperar el mensaje $m \equiv qq^{'}s + pp^{'}t \pmod{N}$.

En el punto tres se obtiene el mensaje m al resolver el sistema de congruencias del punto dos.

Uno de los ataques más utilizados para romper el sistema RSA es el de factorizar n, y existen diferentes formas de hacerlo, así como otras maneras de tratar de descifrar el mensaje sin conocer la factorización de n (cf. [25]).

A continuación se muestra la implementación del sistema de cifrado RSA con SAGE.

Como la operación que se realiza para el cifrado de un mensaje es la exponenciación modular, se utiliza el siguiente algoritmo para realizar dicha operación.

```
sage: def potenciaRSA(b,k,n):
...       #Funcion que calcula b^k mod n
...       d=1
...       c=0
...       lista=integerdigits(k,2)
...       a=len(lista)
...       for i in range(a):
...           c=2*c
...           if d==1:
...               d=1
...           if d!=1:
...               d=(d^2)%n
...           if lista[i]==1:
...               c=c+1
...               d=(d*b)%n
...       return d
```

Para cifrar un mensaje se considera la elección de los números primos entre 10^{180} y 10^{200}.

```
sage: #RSA
sage: def cifradoRSA(m):
...       p=random_prime(10^180,10^200)
...       q=random_prime(10^180,10^200)
...       n=p*q
...       f=(p-1)*(q-1)
...       e=randint(2,f)
...       gc1=gcd(e,f)
```

```
...       while gc1!=1:
...           e=randint(2,f)
...           gc1=gcd(e,f)
...       print "n = ",n
...       print "e = ",e
...       c=potenciaRSA(m,e,n)
...       print "El mensaje cifrado es: ",c
...       d=inversomult(e,f)
...       print "d = ",d
...       print "El mensaje descifrado es: ",potenciaRSA(c,d,n)
```

Ejemplo 13. Supóngase que se desea cifrar el mensaje $m = 4734325412123234234234$, como resultado de cifradoRSA(m) se obtiene:

```
sage: cifradoRSA(4734325412123234234234)

n = 5105438092100728091741916334830888598571999685339679946198421765670747
5886164647840970064671283946542652298282456327501999378876899041538886265 1
8764616099976959842445476399579175488048784183779625031724044312621005440 1
6838099267723893338357489968003018662852066722191603825568826471825106793 6
8701387899686655383788675154619386049381916920982583660788898553700 3

e = 5807745015415216812642973952052971281089147817747820581121874685286115
8992361517870868243946089572831957721632734296214800064970765453789846017 1
9725671064693492100814138250921186543398949350826095035374856326742386237 3
3603104475541802543674410697942548659993443735183406110691420334357405586 2
8092893464121815133435990580651964088675431686095322429880893584573

El mensaje cifrado es:
6394295366626499335051469004574362753496859991451940866178823267161871597 9
2629289987077153753288700142639528800583601448769685639730846140439970846 9
1283299458231917068980995661449638398806867768634871128819760038600671826 0
0863108451627346782005640072665554564770673182895157285087956912758456986 7
6304018423838327804958529577541291115107911229754625770724870 36

d = 1775117024435117492664406332823602720954470065037111537840677924351427
9057773005420622487397515760923337889579084923788439753053641520528006208 6
2399226535990553643561739709234115700038928681048460709334181507042687943 4
6789249979330448690505076811344693076547272445096657765154713890509760314 8
8675554550285676729415282297942210957067335790149373155211031658136 5

El mensaje descifrado es:  4734325412123234234234
```

Existen algoritmos mas eficientes que los mostrados en este apéndice que hacen más rápido el cifrado o descifrado para el sistema RSA, así como se muestra en [4], escrito por Günther Brandner y publicado en enero del 2013.

Apéndice B

Función hash SHA-3

En este apéndice se describe brevemente la función SHA-3 que se menciona en el capítulo 5. Para una descripción detallada puede consultarse [3].

Una función hash asocia a cada cadena finita una cadena de longitud fija. Tales funciones se utilizan, entre otras cosas, para verificar la autenticidad de documentos, almacenando en forma segura el hash del documento.

El hash de una cadena se conoce también como huella digital, y en la práctica es una cadena binaria de aproximadamente 160 bits.

Dada una función hash $h : \mathcal{M} \to \mathcal{T}$ debe ser computacionalmente imposible resolver alguno de los siguientes problemas:

Preimagen Para $t \in \mathcal{T}$ encontrar $m \in \mathcal{M}$ tal que $h(m) = t$.

Una función hash para la que no puede resolverse este problema se dice de una vía o resistente a preimágenes.

Segunda Preimagen Para un $m \in \mathcal{M}$, encontrar $m' \in \mathcal{M}$, $m' \neq m$ tal que $h(m') = h(m)$.

Cuando no puede resolverse este problema h se dice resistente a segunda preimagen.

Colisión Encontrar $m, m' \in \mathcal{M}$ tales que $h(m) = h(m')$ con $m \neq m'$.

Cuando no puede resolverse este problema h se dice resistente a colisiones.

B.1. Funciones esponja

Las funciones esponja fueron desarrolladas por Bertoni, Daemen, Peeters y Van Assche para estudiar la seguridad de las funciones hash.

Internamente las funciones esponja operan bloques de longitud fija b llamados estados. La esponja comprime los datos en lo que se denomina la fase de absorción y entonces extrae datos de longitud arbitraria en la fase de exprimido.

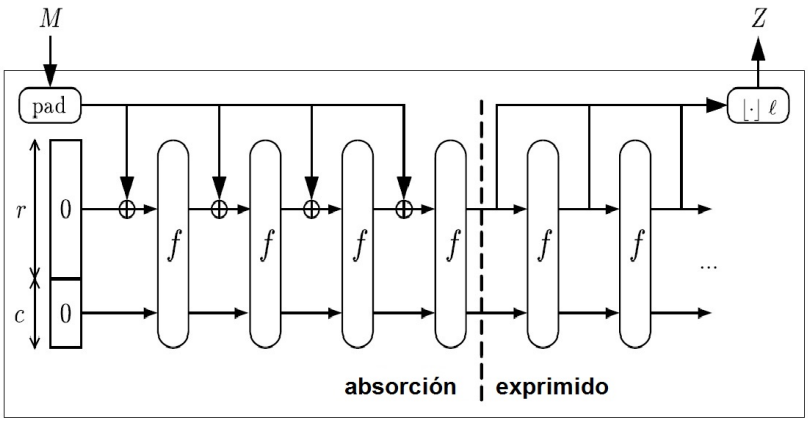
A partir de una entrada con longitud variable, se obtiene como resultado una salida de longitud variable basada en una permutación f, llamada función subyacente, operando en b bits. Este número de bits se obtiene como la suma de dos parámetros r y c de la función esponja.

El algoritmo funciona de la siguiente manera: inicialmente la cadena de entrada es rellenada con bits extras y dividida en bloques de bits de longitud r. Entonces los b bits de estado son inicializados a 0, momento en el cual se inician las dos fases "absorción" y "exprimido".

- En la fase de *absorción*, a los bloques de entrada de longitud r-bits se les aplica un XOR con los primeros r bits del estado, alternándose con la función f. Cuando todos los bloques han sido procesados, se pasa a la siguiente fase.
- Para la fase de *exprimido*, los primeros r bits del estado son devueltos como bloques de salida, alternándose con ejecuciones de la función f. El número de bloques de salida es seleccionado por el usuario.

Los últimos c bits de estado no se ven afectados directamente por los bloques de entrada y no se emiten durante la fase de exprimido.

La siguiente figura nos muestra en modo gráfico a la función esponja, donde por cuestiones de espacio la operación de relleno de denota como pad, M es el mensaje original, $\lfloor \cdot \rfloor_\ell$ denota el truncado de la cadena binaria a sus primeros ℓ bits y Z es el resultado de aplicar la función esponja al mensaje M.



En contraste con otras construcciones la esponja descansa en los parámetros ajustables c y r, que tienen impacto directo en el desempeño del algoritmo.

El parámetro r afecta la velocidad del algoritmo determinando el tamaño de los bloques en el cual se dividen los datos rellenados. Esto hace a la esponja aplicable a una variedad de situaciones donde la velocidad puede ser de importancia. Otra característica deseable en la construcción esponja es la habilidad de producir salidas de longitud arbitraria, por lo que sólo se requiere un algoritmo para la mayoría de las necesidades hash.

En [2] se encuentra una exposición detallada de las funciones esponja, en particular se prueba que el parámetro c tiene un impacto sobre la seguridad de la función.

B.2. SHA-3

El 2 de noviembre de 2007 NIST (Instituto Nacional de Normas y Tecnología de EU) anunció un plan para desarrollar el SHA-3. Se recibieron 64 propuestas para el 31 de octubre del 2008. En la primera ronda, en diciembre del 2008 se seleccionaron 51 de ellas, en junio del 2009 fue la segunda ronda y se seleccionaron sólo 14 candidatos, el 9 de noviembre de 2010 NIST anunció los 5 finalistas que ganaron la tercera ronda. El 2 de octubre del 2012 se anunció al ganador: KECCAK.

El SHA-3 (cf. [3]) fue desarrollado por:

- Guido Bertoni (STMicroelectronics, Italia).
- Joan Daemen (STMicroelectronics, Bélgica).
- Michael Peeters (NXPSSemiconductors, Bélgica).
- Gilles Van Assche (STMicroelectronics, Bélgica).

Keccak es una familia de funciones hash que están basadas en la construcción esponja, y de ahí es una familia de funciones esponja.

En Keccak, la función subyacente es una permutación elegida de entre siete permutaciones fijas. Tales funciones se denotan como SHA-3-$f[b]$ con b en $\{25, 50, 100, 200, 400, 800, 1600\}$. En todos los casos b denota el número de bits del estado, esto es SHA-3-$f[b]$: $\mathbb{Z}_2^b \to \mathbb{Z}_2^b$ con los bits numerados de 0 a $b-1$. Cada estado es organizado como un arreglo binario de tamaño 5×5, cada uno de longitud $w \in \{1, 2, 4, 8, 16, 32, 64\}$, tal que $w = \frac{b}{25}$.

Si S es el estado interno visto como vector de longitud b y A es cuando se ve como paralelepípedo, entonces

$$S[w(5y + x) + z] = A[x, y, z]$$

con $x, y \in \mathbb{Z}_5$, $z \in \mathbb{Z}_w$.

El mensaje original $m \in \mathcal{M}$ se rellena como $m||relleno(m)$, donde se define $relleno(m) = 10^\alpha 1$ y α es un entero, $0 \leq \alpha \leq r - 1$, tal que la longitud de $m||relleno(m)$ es un múltiplo de r.

El estado interno se inicializa en ceros $A[x, y, z] = 0$ para todo x, y, z, $S = 0, S \in \mathbb{Z}_2^b$.

Permutaciones SHA-3-$f[b]$:

En la función esponja utilizada por SHA-3 las fases de absorción y exprimido dependen de una función biyectiva:

$$Ronda : \mathbb{Z}_2^b \to \mathbb{Z}_2^b$$

con $b = r + c$, donde r y c se eligen arbitrariamente.

La función subyacente de SHA-3, denotada SHA-3-$f[b]$, es una permutación iterada, consistente de $n_r = 12 + 2\log_2\left(\frac{b}{25}\right)$ rondas de la función *Ronda*, indexadas con i_r de 0 a $n_r - 1$. Una ronda consiste en la evaluación de $Ronda(A) = \iota \circ \chi \circ \pi \circ \rho \circ \theta(A)$, donde ι es la única función distinta en cada ronda. Las funciones componentes de *Ronda* se definen enseguida:

Denotamos como a el estado interno anterior y como A el nuevo estado.

θ: $A[x, y, z] \leftarrow a[x, y, z] + \sum_{y' \in \mathbb{Z}_5} a[x - 1, y', z] + \sum_{y' \in \mathbb{Z}_5} a[x + 1, y', z - 1]$.

θ se elige por su alta difusión, es decir modifica una alta cantidad de bits, es sencilla de implementar, y por su acción con χ cada bit de entrada potencialmente modifica 31 bits de salida.

ρ: $A[x, y, z] \leftarrow a\left[x, y, z - \frac{(t+1)(t+2)}{2}\right]$, con $t = -1$ si $x = y = 0$ y $0 \leq t \leq 23$ es tal que

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}^t \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

en otro caso. Las operaciones se realizan módulo 5.

ρ hace que la difusión entre las rebanadas[1] sea muy rápida.

π: $A[x, y, z] \leftarrow a[x', y', z]$, donde

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

y las operaciones se realizan módulo 5.

π permuta los carriles[2], y produce dispersión entre rebanadas.

χ: $A[x] \leftarrow a[x] + (a[x + 1] + 1)a[x + 2]$, en esta función y, z toman cualquier valor.

χ se eligió por su sencillez algebraica, por el bajo costo computacional, y además porque propaga rápidamente la no linealidad. Por ser la única función no lineal, es la que le da la no linealidad a la función SHA-3-f.

[1] Bits del estado con la misma coordenada z.

[2] Bits del estado con las mismas coordenadas x, y.

ι**:** $A \leftarrow a + RC_{i_r}$, con $RC_{i_r} \in \mathbb{Z}_2^{5\times5\times w}$ definido como

$$\begin{aligned} RC_{i_r}[0,0,2^j-1] &= rc[j+7i_r], 0 \leq j \leq \frac{w}{2} \\ RC_{i_r}[x,y,z] &= 0 \text{ en otro caso.} \end{aligned}$$

y $rc[t] = (x^t \text{ mód } x^8 + x^6 + x^5 + x^4 + 1) \text{ mód } x$, i_r es el número de ronda.

ι rompe cualquier simetría y punto fijo, aunque actúa en un único carril, θ y χ distribuyen las modificaciones en todos los carriles.

La función esponja para SHA-3:

Se construye la función $Esponja[m, f, relleno, r]$, donde m es una cadena binaria finita, f es una función dada, $relleno$ es una función que agrega una cadena de bits a cada entrada a fin de obtener una longitud múltiplo de r, con r un entero positivo. La función SHA-3 será una evaluación de Esponja en algunas de las funciones y parámetros ya discutidos.

Para el algoritmo de la función Esponja se utiliza la siguiente notación: x es una cadena de bits, $|x|$ es su número de bits, y $|x|_d = \lceil |x|/d \rceil$, donde $\lceil \cdot \rceil$ es el menor entero mayor o igual a x. Además se utiliza $\lfloor x \rfloor_d$ para representar el truncado de la cadena binaria x a sus primeros d bits.

Algoritmo Esponja (Versión 3.0).
Entrada: $m, f, relleno, r, b$ (con $r < b$)
1. $P = m\|\|relleno(m)$, con $P = P_0\|\| \ldots \|\|P_{k-1}$ y $k = \|P\|_r$
2. $s = 0^b$, $c = b - r$, $\ell = c/2$
3. Para $i = 0$ hasta $k - 1$
3.1 $s = s \oplus (P_i\|\|0^{b-r})$
3.2 $s = f(s)$
4. $Z = \lfloor s \rfloor_r$
5. Mientras $\|Z\|_r r < \ell$
5.1 $s = f(s)$
5.2 $Z = Z\|\| \lfloor s \rfloor_r$
Salida: $\lfloor Z \rfloor_\ell$

En este algoritmo cada P_i, $0 \leq i \leq k-1$, tiene longitud r. La función SHA-3 se define entonces como:

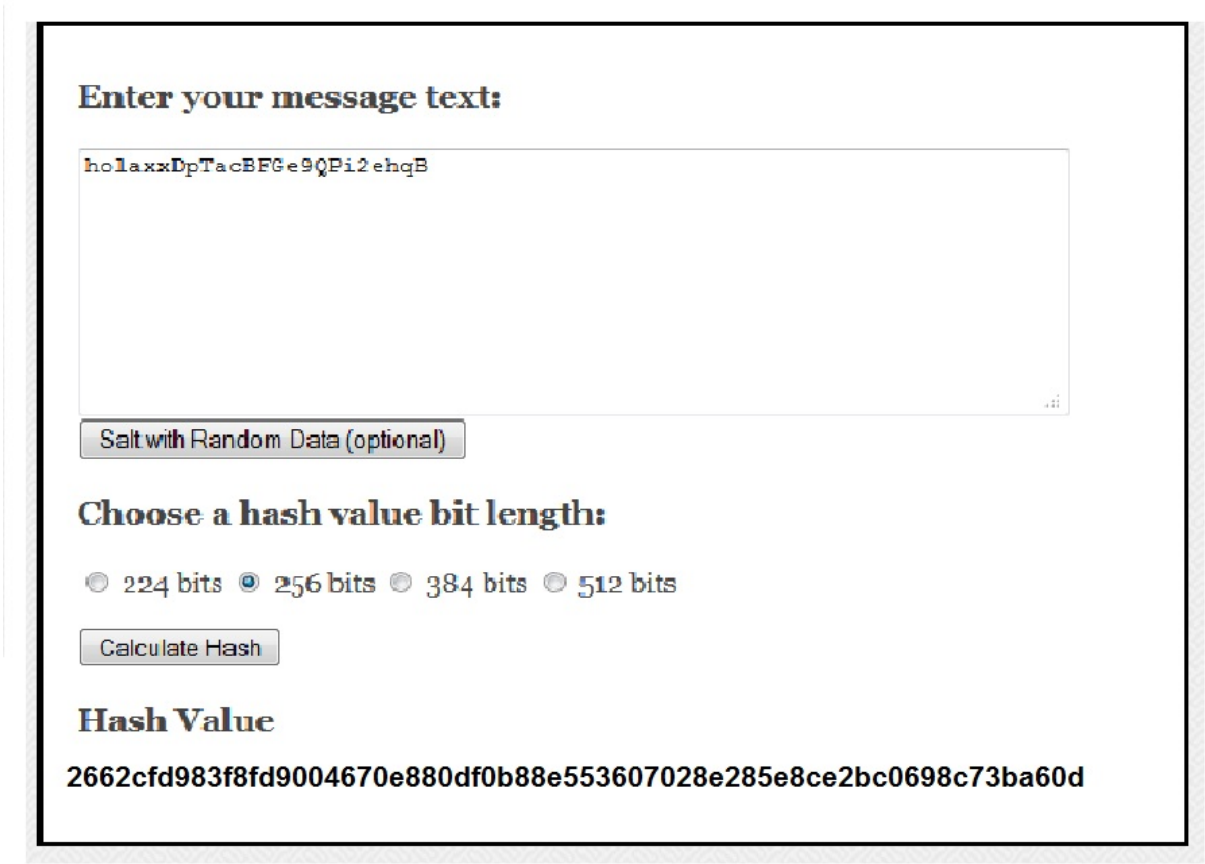
$$\text{SHA-3}[m, r, c] = Esponja[m, \text{SHA-3-}f[r + c], relleno, r]$$

donde $0 < r < b$, $r + c = b$ es un valor válido y $relleno$ es la función definida en la página 107.

Algunos valores recomendados para r y c se presentan en la siguiente tabla:

r	c	Longitud de la salida $\ell = c/2$
1152	448	224
1088	512	256
832	768	384
576	1024	512

En [30] se puede calcular el SHA-3 de un mensaje donde se puede elegir la longitud de la salida, como podemos ver en la siguiente figura:



Para mayores detalles de la función SHA-3 se puede consultar [3].

Apéndice C

Puntos fijos de $D_k(x, a)$

En este apéndice se presentan resultados que se utilizan en el capítulo 4 relacionados a puntos fijos, además de su definición y algunas otras aplicaciones a la criptografía.

Definición 7. *Sea $f : A \to B$ una función de A en B, $c \in A$ es un punto fijo de $f(x)$ si y sólo si $f(c) = c$.*

Así para un polinomio de Dickson de grado k, $D_k(x, a)$, un punto fijo es un elemento c tal que $D_k(c, a) = c$.

El número de puntos fijos de una función incrementa bajo la composición de funciones, y para las aplicaciones en particular el cifrado de Dickson que se describe en el capítulo 4, se desea tener polinomios de permutación con el menor número de puntos fijos.

A continuación se determinará el número de puntos fijos de $D_k(x, a)$.

Teorema C.1. *Sea $fij(\mathbb{F}_q, D_n, a)$ el número de puntos fijos de $D_n(x, a)$ sobre $\mathbb{F}_q$. Si $\mathbb{F}_q$ tiene característica p y $n \geq 1$ entonces*

$$fij(\mathbb{F}_q, D_n, 1) = \frac{1}{2}\left[(q+1, n+1) + (q-1, n+1) + (q+1, n-1) + (q-1, n-1)\right] - \epsilon_1$$

donde

$$\epsilon_1 = \begin{cases} 1, & \textit{si } p \textit{ es impar y } n \textit{ es par,} \\ 2, & \textit{si } p \textit{ y } n \textit{ son impares.} \end{cases}$$

Demostración. Por la proposición 4.2, el conjunto M de todas las soluciones de las ecuaciones $z^2 - rz + 1 = 0$ en $\mathbb{F}_{q^2}$ es $M = K \cup L$, donde $K = \langle \omega^{q+1} \rangle$, $L = \langle \omega^{q-1} \rangle$ y ω es un generador de $\mathbb{F}_{q^2}$.

Notemos que $u \in K \cap L$ si y sólo si $u = \pm 1$, pues si $u \in K \cap L$ entonces $u^{q+1} = 1$ y $u^{q-1} = 1$ de donde $u^q = u$ y así $u^2 = 1$, de esta manera $u = \pm 1$; y si $u = \pm 1$ se satisface $u^{q+1} = u^{q-1} = 1$.

Sea $N_3 = \{1\}$ si $p = 2$ y $N_3 = \{\pm 1\}$ si p es impar, y sea $N_1 = K \backslash N_3$ y $N_2 = L \backslash N_3$. Notemos que M es la unión ajena

$$M = N_1 \cup N_2 \cup N_3.$$

Finalmente si u es una solución de $z^2 - rz + 1 = 0$, también lo es u^{-1}, y $u = u^{-1}$ si y sólo si $u^2 = 1$, esto es $u \in N_3$.

El elemento $x = u + u^{-1}$ es un punto fijo de $D_n(x, 1)$ si y sólo si $u^n + u^{-n} = u + u^{-1}$ lo que es equivalente a

$$(u^{n+1} - 1)(u^{n-1} - 1) = 0. \tag{C.1}$$

Como una solución v de (C.1) es una solución de $u^{n+1} = 1$ y $u^{n-1} = 1$ si y sólo si $v \in N_3$, el número de soluciones de (C.1) sobre M es la suma de los números de soluciones de $u^{n+1} = 1$ y $u^{n-1} = 1$ sobre N_1 y N_2 más el número de soluciones de (C.1) sobre N_3.

Ahora $v \in K$ es una solución de $u^{n+1} = 1$ si y sólo si $r(n + 1) \equiv 0 \pmod{(q + 1)}$. Esta congruencia tiene $(q+1, n+1)$ soluciones. Similarmente $u^{n+1} = 1$ tiene exactamente $(q - 1, n + 1)$ soluciones en L, $u^{n-1} = 1$ tiene exactamente $(q + 1, n - 1)$ soluciones en K y $u^{n-1} = 1$ tiene exactamente $(q - 1, n - 1)$ soluciones en L. También notemos que (C.1) tiene exactamente una solución si $p = 2$ o p es impar y n es par, y tiene exactamente dos soluciones cuando p y n son impares. Así (C.1) tiene ϵ_1 soluciones sobre N_3. Además si u es una solución de (C.1) también lo es u^{-1} por lo que

$$fij(\mathbb{F}_q, D_n, a) = \frac{1}{2}\left[(q + 1, n + 1) + (q - 1, n + 1) + (q + 1, n - 1) + (q - 1, n - 1)\right] - \epsilon_1$$

□

Hay muchas aplicaciones en las que se necesita encontrar números primos grandes. Una prueba de primalidad es una condición para decidir si un número n es o no primo. Si n pasa una prueba de primalidad, es decir, n satisface un criterio determinado, entonces n puede ser primo. Un pseudoprimo n es un número que pasa una prueba de primalidad no determinística en particular.

Definición 8. *Si n es un número impar y b es un entero tal que*

$$b^n \equiv b \ (mód\ n) \tag{C.2}$$

entonces n es llamado un pseudoprimo para la base b, abreviando $psp(b)$.

Si n es primo, entonces para cualquier b se satisface la ecuación (C.2) por el pequeño teorema de Fermat. Pero si n no es primo, todavía es posible, pero no es muy probable que (C.2) se cumpla para una b elegida al azar. Es aún menos probable que (C.2) se cumpla para todos los números enteros b. Un entero compuesto impar n tal que (C.2) se cumple para cada número entero b se llama un *número de Carmichael*. Se puede demostrar que un entero compuesto impar n es un número de Carmichael si y sólo si n es libre de cuadrados

y $(p-1)|(n-1)$ para cada primo p que divide a n (cf. [5]). El número más pequeño de Carmichael $n = 561 = 11 \cdot 03 \cdot 17$.

Un entero b que satisface (C.2) se llama *testigo para la primalidad de* n. Testigos falsos, números que satisfacen (C.2) para n compuesto, dan lugar a pseudoprimos que son números compuestos y si todo b es testigo sin ser n primo, entonces n es un número de Carmichael. La siguiente definición es una generalización de pseudoprimos.

Definición 9. *Un entero n impar que satisface*

$$D_n(b, c) \equiv b \ (mód\ n) \tag{C.3}$$

es llamado un pseudoprimo de Dickson de clase (b, c), abreviando $Dpsp(b, c)$.

De la definición de polinomios de Dickson de primer orden la congruencia (C.3) se satisface para todo número primo n y para cualquier $b \in \mathbb{Z}$. Si se considera $c = 0$ entonces (C.3) se reduce a (C.2). Una prueba de pseudoprimos de Dickson trabaja de manera similar a las pruebas probabilísticas de primalidad.

Definición 10. *Un entero impar n es llamado un pseudoprimo fuerte $c - Dickson$ si se satisface (C.3) para todos los enteros b y un entero fijo c.*

Los pseudoprimos fuertes $0 - Dickson$ son los números de Carmichael.

Apéndice D

Algoritmos en SAGE

En este apéndice se muestran los algoritmos del capítulo 4, implementados en SAGE de manera análoga a los algoritmos implementados en Mathematica, tanto para el cifrado de datos basado en polinomios de Dickson como para los ataques.

D.1. Cifrado de Dickson

Los algoritmos necesarios para realizar el cifrado de datos son los siguientes:

Algoritmo 1

Para este algoritmo se requiere de una función que en SAGE no está implementada como se requiere, por lo que fue necesario hacer una función que devuelva la representación de un número en una base dada.

```
sage: def integerdigits(a,b):
...       # da el valor de a en base b
...       c=a
...       lista=[0]
...       while c!=1:
...           c=floor(a/b)
...           lista.append(a%b)
...           a=c
...       lista.append(1)
...       lista=lista[1:len(lista)]
...       l=len(lista)
...       listas=[0 for i in range(l)]
...       for i in range(l):
...           listas[i]=lista[l-1-i]
...       return listas
```

Este algoritmo calcula la potencia de $(u^k \text{ mód } u^2 - ub + 1) \text{ mód } n$.

```
sage: def potenciadickson(n,k,b):
...       #Funcion que calcula la potencia (u^k mod u^2 -ub + 1)mod n
...       R=IntegerModRing(n)
...       T=PolynomialRing(R,'u')
...       u=T.0
...       f=u^2-b*u+1
...       d=1
...       c=0
...       lista=integerdigits(k,2)
...       a=len(lista)
...       for i in range(a):
...           c=2*c
...           if d==1:
...               d=1
...           if d!=1:
...               d=(d^2)%f
...           if lista[i]==1:
...               c=c+1
...               d=(d*u)%f
...       return d
```

Algoritmo 2

Evalúa el polinomio de Dickson de grado k en b módulo n.

```
sage: def evpoldickson(n,k,b):
...       # Funcion que evalua el polinomio de dickson en b.
...       pold=potenciadickson(n,k,b)
...       coef=pold.coeffs()
...       if pold in ZZ:
...           a0=coef[0]
...           a1=0
...       if  not pold in ZZ:
...           a0=coef[0]
...           a1=coef[1]
...       return ((a1*b + 2*a0)%n)
```

El siguiente algoritmo cifra un mensaje dado m. Elige aleatoriamente los factores primos p_i, $i = 1, 2$ de n donde cada factor está entre 10^{80} y 10^{90}, también elige aleatoriamente el valor de la llave de cifrado k.

```
sage: #funcion que cifra el mensaje dado m
sage: #se imprime n,k,c
sage: def cifrar(m):
...       p=random_prime(10^80,10^90)
...       q=random_prime(10^80,10^90)
...       n=p*q
...       a=lcm(p^2-1,q^2-1)
...       k=randint(2,a)
...       gc=gcd(k,a)
...       while gc!=1:
...           k=randint(2,a)
...           gc=gcd(k,a)
...       print "n = ",n
...       print "k = ",k
...       print "El mensaje cifrado es c = ",evpoldickson(n,k,m)
```

En seguida se ilustra el tipo de salida que se obtiene al evaluar la función cifrar.

Ejemplo 14. `sage: cifrar(472547215744714231234123423428923462887588757464 3462754872354724)`

```
n = 260199147940962133275986764523459256459494496523558223305185725924428
516609200372199477612581020095584481012878108085169480111784362762425026 4
122125841853485079

k = 691221180367641630122311732998129525891184051609562001733377181982479
464381673175019924042302549042576435470725330145406718978690899512385532 2
562460857075208650388796650520601867042801904604092206391585035979043428 4
748748171895570970930231458161088202405902040106234670080629635462443732 7
109971531469460362900394873 91

El mensaje cifrado es c = 181677995650243709873030254533134965973383623 27
141813101774758451514831666315075005708031185292815682468390752045495702 2
475699257915990541692461612766545 1900059
```

D.2. Ataques

En esta sección se presentan los algoritmos con los que se realizan los ataques al cifrado de Dickson.

D.2.1. Algoritmo para el descifrado parcial

Se muestran los algoritmos necesarios para hacer el descifrado parcial de un mensaje que está cifrado con el sistema basado en polinomios de Dickson.

Algoritmo 3

```
sage: # algoritmo para factorizar s
sage: def factors(k,s):
...       s1=1
...       s2=s
...       mcd=(s2).gcd(k)
...       while mcd>1:
...           s1=s1*mcd
...           s2=s2/mcd
...           mcd=(s2).gcd(k)
...       return s

sage: #algoritmo que calcula k^(-1)mod n
sage: def inversomult(k,n):
...       (d,u,v)=xgcd(k,n)
...       if d!=1:
...           print k," no tiene inverso multiplicativo modulo ",n
...       if d==1:
...           if u>0:
...               return u
...           if u<0:
...               return (-u)
```

Algoritmo 4

```
sage: # algoritmo descifrado parcial
sage: # n es el modulo, k el grado del polinomio y c el texto cifrado
sage: def descifradoparcial(n,k,c):
...       s=1
...       while s<100000 and evpoldickson(n,s,c)!=2:
...           s=s+1
...       if evpoldickson(n,s,c)!=2:
...           print "Algoritmo sin exito"
...       if evpoldickson(n,s,c)==2:
...           s1=factors(k,s)
...           s2=s/s1
```

```
...           ka=inversomult(k,s2)
...           m=evpoldickson(n,ka,c)
...           print "El mensaje original es m=",m
```

D.2.2. Algoritmo para encontrar la factorización de n.

En esta sección presentamos los algoritmos para poder realizar el ataque, en el que en caso de ser exitoso se encuentra la factorización de n.

Algoritmo 5

```
sage: #algoritmo que calcula v_2(s)
sage: def V2(s):
...       e=1
...       while s%(2^e)==0:
...           e=e+1
...       m=e-1
...       return m
```

Algoritmo 6

```
sage: #algoritmo que calcula jmax
sage: def JMAX(c,n,s,g):
...       for r in range(g):
...           if evpoldickson(n,s/(2^r),c)==2:
...               max=r
...       return max
```

Algoritmo 7

```
sage: #algoritmo que dados n y c, en caso de ser posible regresa la
factorizacion de n

sage: def factorizacion(n,c):
...       s=2
...       while s<100000 and evpoldickson(n,s,c)!=2:
...           s=s+2
...       if evpoldickson(n,s,c)!=2:
...           print "Algoritmo sin exito"
...       v2=V2(s)
...       j=JMAX(c,n,s,v2)
...       if j==v2:
```

```
...             print "Algoritmo sin exito"
...         if j!=v2:
...             dic=evpoldickson(n,s/(2^(j+1)),c)
...             if dic==-2:
...                 print "Algoritmo sin exito"
...             if dic!=-2:
...                 d=xgcd(dic-2,n)
...                 d2=n/d[0]
...                 print n," = ",d[0]," * ",d2
```

Resultados

En este trabajo de tesis dos de los resultados más importantes que se obtuvieron fueron el lema 2.7 y el teorema 2.12. A este último se le añadieron algunas condiciones para que el resultado fuera válido, pues como aparecen en el artículo [28] se encontraron contraejemplos, uno de ellos es el ejemplo 5. Al hacer la revisión de [28], el lema 2.7 se utiliza para demostrar el teorema 2 de [28], el cual es un caso particular del teorema 2.12, por lo que el contraejemplo para el lema 3.3 también los es para el teorema 2 de [28].

El teorema 2.12 es muy importante para el desarrollo del presente escrito, pues el sistema de cifrado descrito y el protocolo de intercambio de claves están basados en los polinomios de permutación de Dickson. Si se utiliza el resultado como aparece en [28] se pueden encontrar polinomios de permutación de Dickson para los cuales no se pueda determinar su inversa, bajo la operación de composición, lo que no garantiza el descifrado del mensaje.

Otro resultado importante es el lema 2.7, el que resultó al hacer correcciones al lema 5 de [24]. Tales correcciones fueron necesarias pues se le encontraron contraejemplos, uno de ellos es el ejemplo 2, resultando así el lema 1.13. La importancia de este resultado es que se utiliza para demostrar el teorema 1.14 (se da una demostración alternativa en teorema 1.17), mismo que se utiliza en la demostración del lema 2.7. Esta cadena de resultados es fundamental en el presente trabajo.

El sistema de cifrado propuesto en este trabajo es importante pues se puede utilizar en lugar del RSA. Se demostró que el sistema de cifrado basado en polinomios de Dickson es al menos tan seguro como el sistema RSA, y su seguridad se basa también en el problema de factorización de enteros.

El protocolo de intercambio de claves propuesto en [28] está basado en el teorema 2 que aparece en ese artículo, el cual es falso. Por lo que el protocolo presentado en el presente trabajo está basado en el resultado obtenido del teorema 2.12, es decir en polinomios de permutación de Dickson de grado impar y no múltiplos de 3. Además la función hash que se propone utilizar en el protocolo de intercambio de claves basado en polinomios de Dickson es SHA-3, función aceptada como ganadora el 2 de octubre de 2012.

En el cuadro 4.1 se muestran los tiempos de ejecución de algunos mensajes que fueron cifrados con RSA y el sistema de cifrado basado en polinomios de Dickson, en el que se puede notar que en los tiempos de ejecución de los algoritmos implementados para RSA y el cifrado de Dickson no hay mucha diferencia, y se confirma por que RSA es el más usado en la práctica.

Conclusiones

El sistema de cifrado basado en polinomios de permutación de Dickson resuelve uno de los problemas más importantes de la criptografía: la transmisión de mensajes de forma segura, siendo una alternativa al uso del sistema RSA.

Hoy en día el sistema RSA, es el estándar de comunicación electrónica segura más usado. En este trabajo se propone un sistema para cifrar datos basado en polinomios de permutación de Dickson, del cual se analizó su seguridad y se dieron las condiciones para garantizarla. Además su seguridad se basa, al igual que RSA, en el problema de factorización de enteros. En ambos criptosistemas las operaciones se realizan en $\mathbb{Z}_n$, donde $n = p_1 p_2$, con p_1 y p_2 primos impares distintos. Para poder encontrar la clave de descifrado, es necesario conocer la factorización de n para poder calcular $\varphi(n)$ y $v(n)$, respectivamente, como se definió en el apéndice A y (2.30).

El intercambio de claves entre usuarios de una red de comunicación también es uno de los problemas más importante de la criptografía, así que una propuesta a la solución de este problema es el protocolo de intercambio de claves basado en polinomios de Dickson que se analiza en este trabajo.

Se estudia también la seguridad del protocolo de intercambio de claves utilizando polinomios de Dickson, la cual está basada principalmente en que no es posible resolver el problema de Dickson discreto, análogo al problema del logaritmo discreto.

El protocolo de intercambio de claves que se presenta aquí, es una mejora del que aparece en [28]; pues como ya se mencionó los resultados en los que se basa son falsos. Se hicieron algunas correcciones a dichos resultados, y las adaptaciones correspondientes al protocolo propuesto, además que ya se mencionó el uso de la nueva función hash estándar (SHA-3).

Se concluye que la revisión de artículos debe hacerse de manera cuidadosa, pues aun en aquellos publicados en las revistas de prestigio se pueden encontrar errores.

Perspectivas

Con la revisión de lecturas acerca del polinomio de Dickson se encontraron algunas aplicaciones interesantes, una de ellas se mencionó en el apéndice de puntos fijos de $D_k(x, a)$. Las pruebas de primalidad que se hacen basándose en polinomios de Dickson, abordan uno de los problemas más importantes para la teoría de números y la criptografía. Los pseudoprimos de Dickson se introdujeron por primera vez en [16] como una generalización de los pseudoprimos de Fibonacci y Lucas, y se pueden buscar nuevas pruebas de primalidad usando polinomios de Dickson.

Hay una serie de polinomios en una o varias variables que son similares a los polinomios Dickson, o están directamente relacionados con ellos a través de una relación matemática (cf. [13]). También hay una función racional que está conectada con los polinomios de Dickson de primer orden, que presentó por primera vez L. Rédei en [22], y se conocen como funciones Rédei. Existen sistemas de cifrado basados en polinomios de Dickson en varias variables y funciones Rédei, los cuales fueron estudiados por Lidl y Muller en [14] y [15]. En este sentido como tema de investigación se pueden hacer el análisis de los sistemas de cifrado, así como de su seguridad. En base a polinomios de Dickson en varias variables o funciones Rédei se pueden proponer nuevos protocolos de intercambio de clave y firma digital, que hasta el momento no se han encontrado en la literatura existente.

Las funciones bent son funciones booleanas, es decir funciones binarias definidas sobre $\mathbb{Z}_2^n$, que están lo más alejadas posibles de las funciones lineales, en cierta comparación de cercanía (métrica de Hamming) cf. [6]. Son importantes en varios aspectos de la criptografía, y no se han clasificado mas allá de $n = 6$. Una posible dirección de investigación es estudiar propiedades de funciones hiper-bent (cf. [6]), tratar de generalizar resultados conocidos para funciones bent y obtener nuevos resultados, aplicables en criptografía.

Como los polinomios de Dickson están relacionados con conjuntos diferencia, una opción es estudiar los códigos correctores de errores asociados a tales conjuntos diferencia y tratar de obtener nuevos conjuntos diferencia con funciones hiper-bent (ver [9], [6] y [29]).

Bibliografía

[1] Bergamo P., D' Arco P., De Santis A., Kocarev L. *Security of public-key cryptosystems based on Chebyshev polynomials*. IEEE Trans. Circuits Syst I. **7-52** (2005), 1382 - 1393.

[2] Bertoni G., Daemen J., Peeters M., Van Assche G. *Cryptographic sponge functions*. Versión 01-2011. http://sponge.noekeon.org/CSF-0.1.pdf

[3] Bertoni G., Daemen J., Peeters M., Van Assche G. *The KECCAK reference*. Versión 3.0-2011. http://keccak.noekeon.org/Keccak-reference-3.0.pdf

[4] Brandner G. *RSA, Dickson, LUC and Williams: a study on four polynomial-type public-key cryptosystems*. Applicable Algebra in Engineering, Communication and Computing **24-1** (2013), 17-36.

[5] Carmichael R.D. *On composite numbers P which satisfy the Fermat congruence* $a^P \equiv 1$ *mód* P. American Mathematical Monthly **19** (1912), 22-27.

[6] Charpin, P., Gong G. *Hyperbent functions, Kloosterman sums and Dickson polynomials*. IEEE Trans. Information Theory **54** (2008), 4230-4238.

[7] Dickson L.E. First course in the theory of equations. New York : John Wiley & Sons, 1922.

[8] Diffie W., Hellman M.E. *New directions in cryptography*. IEEE Trans. Information Theory. **22** (1976), 644 - 654.

[9] Flori J., Mesnager S. *Dickson polynomials, hyperelliptic curves and hyper-bent*. SETA, LNCS **7280** (2012), 40-52.

[10] Kocarev L., Tasev Z. *Public-key encryption based on Chebyshev maps*. IEEE Symp. Circuits and Systems (ISCAS 03). **3** (2003), 28-31.

[11] Lausch, H., Muller W. B. and Nöbauer W. *Uber die Struktur einer durch Dicksonpolynome dragestellten Permutationsgruppe des Restklassenringes modulo n*. J. reine angew. Math. **261** (1973), 88 - 99.

[12] Lidl, R. and Niederreiter, H. Finite Fields. Cambridge Univ. Press, 1987.

[13] Lidl, R., Mullen, G. L. and Turnwald, G. Dickson polynomials. Longman Scientific and Technical ; New York : Copublished in the United States with John Wiley & Sons, Harlow, Essex, England, 1993.

[14] Lidl, R., Muller W.B. *Permutation polynomials in RSA-cryptosystems*. Advances in Cryptology. New York 1984, 293-301.

[15] Lidl, R., Muller W.B. *A note on polynomials and functions in algebraic cryptography*. Ars Combin. 17 A (1984), 223-229.

[16] Lidl, R., Muller W.B. *Generalizations of the Fibonacci pseudoprimes test*. Discrete Math. **92** (1991), 211-220.

[17] Menezes A., Oorschot P., Vanstone S.. Handbook of applied Cryptography. 1997.

[18] Muller, W.B., Nobauer W. *Some remarks on public-key cryptosystems*. Studia Sci. Math. Hungar **16** (1981), 71-76.

[19] Muller, W. B., Nobauer R. *Cryptanalysis of the Dickson scheme*. EUROCRYPT'85, LNCS **219** (1986), 50 - 61.

[20] Nobauer, R. *Cryptoanalysis of a public-key cryptosystem based on Dickson polynomials*. Math. Slovaca **38**(1988), 309 - 323.

[21] Nobauer, W. *On the length of cycles of polynomial permutations*. Proc. of the Vienna Conf, Contributions to General Algebra **3** (1984), 265 - 274.

[22] Rédei L. *Uber eindeutig umkehrbare Polynome in endlichen Korpen*. Acta Sci. Math. **11** (1946), 85-92.

[23] Rivest R., Shamir A., Adleman L. *A method for obtaining digital signatures and PKC*. Communications of the ACM **21** (1978), 120 - 128.

[24] Rivest, R.L. *Permutation polynomials modulo* 2^w. Finite Fields and Their Applications **7** (2001), 287-292.

[25] Schnorr, C.P. Zur Analyse des RSA-Schemas. Fachbereich Mathematik, Univ. Frankfurt am Main, 1981.

[26] Shoup, Victor. A Computational Introduction to Number Theory and Algebra. Cambridge Univ. Press, 2005.

[27] Singh, R. P., Saity S. *Permutation Polynomials modulo* p^n. http://eprint.iacr.org/2009/393.pdf

[28] Wei, P., Liao, X., Wong, K. *Key exchange based on Dickson polynomials over finite fields with* 2^m . Journal of Comp. **6** (2011), 2546-2551.

[29] Xiwang C., Weisheng Q. *On Dickson Polynomials and Difference Sets*. Journal of Mathematical Research and Exposition **26** (2006), 219-226.

[30] http://sha3calculator.appspot.com/