# Involuciones de Cuerpos Finitos obtenidos por Binomios

Lillian González Albino

Enero 2018

**Resumen**

Las permutaciones sobre cuerpos finitos son importantes ya que tienen aplicaciones desde cifrados de voz hasta teoría de computabilidad y criptografía. Polinomios que generan permutaciones son llamados **polinomios de permutación**; si estos polinomios son su propia inversa, son llamados **involuciones**. En esta investigación, queremos caracterizar binomios de involución la forma $x^m(x^{\frac{q-1}{2}}+a)$ sobre cuerpos finitos de característica $p$.

## 1. Introducción

Sea $q=p^r$ donde $p$ es primo. Utilizamos $\mathbb{F}_q$ para denotar el cuerpo finito con $q$ elementos, de característica $p$ y $\mathbb{F}_q^*$ para denotar $\mathbb{F}_q\backslash\{0\}$.

Se sabe que los monomios $x$, $x^{q-2}$, y $x^{q-3}$ producen involuciones de $\mathbb{F}_q$ [3]. Para encontrar binomios de involución, un paso razonable es explorar binomios que sean combinaciones de monomios de involución. En nuestra investigación exploramos el binomio de Cáceres y Colón $P_1(x)=x^{q-2}+ax^{\frac{q-3}{2}}=x^{\frac{q-3}{2}}(x^{\frac{q-1}{2}}+a)$ [1] y luego lo generalizamos como $P(x)=x^m(x^{\frac{q-1}{2}}+a)$ con el propósito de caracterizar los binomios de esta forma, es decir buscar condiciones en la $m$ y en la $a$ que sean suficientes y necesarias para que $P(x)$ sea de involución en $\mathbb{F}_q$.

## 2. Preliminares

### 2.1. Raíces Primitivas

Las raíces primitivas nos son útiles para poder representar todos los elementos de $\mathbb{F}_q^*$ de manera abstracta.

**Definición 2.1.1.** Se dice que $\alpha$ es una **raíz primitiva** de $\mathbb{F}_q$ si las potencias de $\alpha$ generan todos los elementos en $\mathbb{F}_q^*$. Es decir, $\mathbb{F}_q^*=<\alpha>=\{\alpha^0,\alpha^1,\alpha^2,...,\alpha^{q-2}\}$.

**Proposición 2.1.1.** Si $\alpha^n=1$ para $n<p-1$, entonces $\alpha$ no es raíz primitiva de $\mathbb{Z}_p$.

*Demostración.* (Contradicción)
Sea $\alpha\in\mathbb{F}_q$. Suponga que $\alpha^n=1$ para $n<q-1$ y que $\alpha$ es raíz primitiva de $\mathbb{F}_q$. Entonces $<\alpha>=\mathbb{F}_q^*$. Note que: $|\mathbb{F}_q^*|=q-1$. Entonces, considere $\alpha^j\in\mathbb{F}_q$, por el algoritmo de división, $j=nd+r$ con $0\leq r<n$ y

$$\alpha^j=\alpha^{nd+r}=(\alpha^n)^d\alpha^r=(1)^d\alpha^r=\alpha^r$$

Por lo tanto, solo hay $0 \leq r < n$ potencias distintas de $\alpha$ y, a lo sumo, obtenemos $n$ elementos distintos como potencias de $\alpha \Rightarrow\Leftarrow$ ya que deben haber $q-1$ elementos distintos como potencias de $\alpha$, por lo tanto, $\alpha$ no es raíz primitiva de $\mathbb{F}_q$. □

**Proposición 2.1.2.** $\alpha$ es raíz primitiva de $\mathbb{Z}_p$ solo si $\alpha^{\frac{p-1}{2}} = -1$.

*Demostración.* (Directa)
Sea $\alpha$ una raíz primitiva de $\mathbb{F}_q$, entonces $q-1$ es el entero más pequeño tal que $\alpha^{q-1} = 1$. Entonces, $\alpha^{q-1} - 1 = 0$. Note que $q$ es impar, por lo tanto, $q-1$ es par y $\frac{q-1}{2} \in \mathbb{Z}$. Ahora,

$$(\alpha^{\frac{q-1}{2}})^2 - 1 = 0 \Rightarrow (\alpha^{\frac{q-1}{2}} - 1)(\alpha^{\frac{q-1}{2}} + 1) = 0 \Rightarrow \alpha^{\frac{q-1}{2}} = \pm 1$$

Pero como $\frac{q-1}{2} < q-1$, $\alpha^{\frac{q-1}{2}} = -1$. □

**Note que.** Si $\alpha^{\frac{q-1}{2}} = -1$, no necesariamente $\alpha$ es raíz primitiva.

*Contraejemplo.* $8 \in \mathbb{Z}_{13}$, $8^{\frac{q-1}{2}} = 8^6 = -1$,y 8 no es raíz primitiva de $\mathbb{Z}_{13}$.

**Proposición 2.1.3.** $\alpha$ es una raíz primitiva de $\mathbb{F}_q$ si y solo si $f : \mathbb{F}_q^* \to \mathbb{F}_q^*$ definido por $f(i) = \alpha^i$ es 1-1 y sobre.

*Demostración.* (Directa)
($\Rightarrow$) Sea *alpha* raíz primitiva. Suponga que $i, j \in \{0, 1, ..., q-2\}$ son tal que $f(i) = f(j) \Rightarrow \alpha^i = \alpha^j \Rightarrow \alpha^{i-j} = 1$. Como $0 \leq i, j \leq q-2$, $0 \leq |i-j| \leq q-2 \Rightarrow i - j = 0 \Rightarrow i = j$. Por lo tanto, $f$ es $1-1$.
Ahora, sea $\beta \in \mathbb{F}_q^*$, entonces $\beta = \alpha^i$ para algún $i \in \{0, 1, ..., q-2\}$. Por lo tanto, $f$ es sobre.
($\Leftarrow$) Suponga que $f : \{0, 1, ..., q-2\} \to \mathbb{F}_q^*$, definida por $f(\alpha^i) = \alpha^i$, una función 1-1 y sobre. Como $f$ es sobre, $\forall\ a \in \mathbb{F}_q^*, a = \alpha^i$ para algún $i \in \{0, 1, ..., q-2\}$. Por lo tanto, $\mathbb{F}_q^* = \{0, 1, ..., q-2\}$ y $\alpha$ es raíz primitiva. □

## 2.2. Residuos Cuadráticos

Muchos de los trabajos con binomios estudiados atan las permutaciones y las involuciones a la reciprocidad cuadrática de coeficientes de los binomios. Es por esto que es importante saber algunas de sus propiedades.

**Definición 2.2.1.** Sea $p$ primo, un entero $a$ es **residuo cuadrático** módulo $p$ si existe $x$ tal que

$$x^2 \equiv a \ mod\ p$$

**Definición 2.2.2.** Sea $p$ primo y $a$ un entero, la función de residuo cuadrático, denotada $\eta(a)$, se define como

$$\eta(a) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a \text{ es un residuo cuadrático módulo p} \\ -1 & \text{si } a \text{ no es un residuo cuadrático módulo p} \end{cases}$$

**Lema 2.2.1.** $\eta(ab) = \eta(a)\eta(b)$

*Demostración.* Sea $\alpha$ raíz primitiva de $\mathbb{F}_q$ y suponga que $a = \alpha^i$ y $b = \alpha^j$. Entonces $ab = \alpha^{i+j}$. Si $\eta(ab) = 1$, entonces

$$i + j \equiv 0 \; mod \; 2 \iff i \equiv j \; mod \; 2 \iff \eta(a) = \eta(b) \iff \eta(a)\eta(b) = 1$$

Si $\eta(ab) = -1$, entonces, por lema, sabemos que $\eta(a) = -\eta(b)$. Esto implica que $\eta(a)\eta(b) = -1$.
Si $\eta(ab) = 0$, entonces por definición tenemos que

$$ab = 0 \iff a = 0 \text{ o } b = 0 \iff \eta(a) = 0 \text{ o } \eta(b) = 0 \iff \eta(a)\eta(b) = 0$$

□

**Lema 2.2.2.** Sean $a, b \neq 0$, $\eta(ab) = -1 \iff \eta(a) = -\eta(b)$.

*Demostración.* (Directa)
($\Rightarrow$) Sean $a, b \neq 0$ y suponga que $\eta(ab) = -1$. Entonces por el lema anterior, sabemos que $\eta(ab) = \eta(a)\eta(b) = -1$. Note que si ambos fuesen 1 o ambos fuesen $-1$, esto implicaría que $\eta(a)\eta(b) = 1$. Note incluso que $a, b \neq 0$, esto implica que $\eta(a) \neq 0$ y $\eta(b) \neq 0$. Por lo tanto el único caso que nos queda es $\eta(a) = 1$ y $\eta(b) = -1$ o $\eta(a) = -1$ y $\eta(b) = 1$. En ambos de estos casos tenemos que $\eta(a) = -\eta(b)$.
($\Leftarrow$) Sean $a, b \neq 0$ y suponga que $\eta(a) = -\eta(b)$. Note que $a, b \neq 0$, esto implica que $\eta(a) \neq 0$ y $\eta(b) \neq 0$. Sin perder generalidad podemos decir que $\eta(a) = 1$ y $\eta(b) = -1$, entonces por el lema anterior sabemos que $\eta(a)\eta(b) = \eta(ab) = -1$. □

**Lema 2.2.3.** Sean $a, b \neq 0$, $\eta(ab) = 1 \iff \eta(a) = \eta(b)$

*Demostración.* (Directa)
($\Rightarrow$) Sean $a, b \neq 0$ y suponga que $\eta(ab) = 1$, por lema sabemos que $\eta(ab) = \eta(a)\eta(b) = 1$. Note que $a, b \neq 0$, por lo tanto $\eta(a) \neq 0$ y $\eta(b) \neq 0$. Si $\eta(a) = -\eta(b)$, por lema anterior tendríamos que $\eta(ab) = -1$, por lo tanto $\eta(a) = \eta(b)$.
($\Leftarrow$) Sean $a, b \neq 0$ y suponga que $\eta(a) = \eta(b)$. Esto se puede dividir en dos casos: $\eta(a) \in \{1, -1\}$. En el caso de que $\eta(a) = 1 = \eta(b)$, tenemos que $\eta(a)\eta(b) = (1)(1) = \eta(ab)$. En el caso $\eta(a) = -1 = \eta(b)$, tenemos que $\eta(a)\eta(b) = (-1)(-1) = \eta(ab)$. En ambos casos tenemos que $\eta(a) = \eta(b)$. □

**Lema 2.2.4.** Sea $a \in \mathbb{F}_q$, $\eta(a) = (a)^{\frac{q-1}{2}}$.

*Demostración.* Suponga que $a \in \mathbb{F}_q$. Sabemos que $\eta(a)$ puede ser $0, 1$, o $-1$. Para el caso $\eta(a) = 0$, $a = 0$, por lo tanto $a^{\frac{q-1}{2}} = 0$. Para el caso $\eta(a) = 1$, tenemos que $a = b^2$ para alguna $b \in \mathbb{F}_q^*$, por lo tanto $a^{\frac{q-1}{2}} = (b^2)^{\frac{q-1}{2}} = b^{q-1} = 1$. Para el caso $\eta(a) = -1$, tenemos que $a \neq b^2$ para ningún $b \in \mathbb{F}_q^*$, por lo tanto $a^{\frac{q-1}{2}} = -1$. □

**Lema 2.2.5.** Sea $b \neq 0$, $\eta(b) = \eta(b^{-1})$

*Demostración.* Sea $\alpha$ raíz primitiva de $\mathbb{F}_q$ y suponga que $b = \alpha^i$. Note que $b^{-1} = \alpha^{-i}$ y que $i \equiv -i \; mod \; 2$. Esto implica que

$$\eta(\alpha^i) = \eta(\alpha^{-i}) \iff \eta(b) = \eta(b^{-1})$$

□

**Lema 2.2.6.** Sea $m$ impar, $\eta(b) = \eta(b^m)$

*Demostración.* Sea $m$ impar y $\alpha$ raíz primitiva de $\mathbb{F}_q$ y suponga que $b = \alpha^i$. Como $m$ es impar, $i \equiv im \ mod \ 2$, esto implica que $\eta(b) = \eta(b^m)$. □

**Lema 2.2.7.** Sea $b \neq 0$, $\eta(ab) = \eta(ab^{-1})$

*Demostración.* Por lema, sabemos que

$$\eta(ab) = \eta(a)\eta(b) = \eta(a)\eta(b^{-1}) = \eta(ab^{-1})$$

□

**Lema 2.2.8.** Sea $m$ impar, $\eta(ab) = \eta(ab^m)$

*Demostración.* Por lema, sabemos que

$$\eta(ab) = \eta(a)\eta(b) = \eta(a)\eta(b^m) = \eta(ab^m)$$

□

## 2.3. Permutaciones

Para que un binomio sea involución en $\mathbb{F}_q$ debe ser una permutación de $\mathbb{F}_q$. Por lo cual es importante saber algunas propiedades de las permutaciones de cuerpos finitos.

**Definición 2.3.1.** Una **permutación** de un conjunto finito $A$ es una función biyectiva de $A$ a $A$.

**Definición 2.3.2.** Un **polinomio de permutación** en $\mathbb{F}_q$ es un polinomio que produce una permutación de $\mathbb{F}_q$.

**Lema 2.3.1.** Sea $A$ un conjunto finito. $f : A \to A$ es $1-1$ si y solo si $f$ es sobre.

*Demostración.* (Directa)
($\Rightarrow$) Suponga que $A$ un conjunto finito y $f : A \to A$ es $1-1$. Como $f$ es función, todo elemento del dominio tiene exactamente uno en la imagen que le corresponde, y como es 1-1 no hay dos elementos del codomino tal que $f(a) = f(b)$ con $a$ distinto de $b$. Por lo tanto, $f$ es sobre.
($\Leftarrow$) Suponga que $A$ un conjunto finito y $f : A \to A$ es sobre. Note que para que todos los elementos en el codominio le corresponde a un elemento en el dominio, por lo tanto $f$ tiene que ser $1-1$. □

**Corolario 1.** Sea $A$ finito, $f : A \to A$ es permutación si y solo si $f$ es 1-1.

*Demostración.* (Directa)
($\Rightarrow$) Sea $A$ finito y suponga que $f : A \to A$ una permutación, entonces todos los elementos en el codominio tienen un elemento correspondiente en el dominio. Por lo tanto, es sobre, y, por el lema anterior, es 1-1.
($\Leftarrow$) Sea $A$ finito y suponga que $f : A \to A$ es $1-1$, entonces $f$ es sobre. Esto dice que $Im(A) = A$. Entonces, $f : A \to A$ es una permutación de $A$. □

**Lema 2.3.2.** Sea $A$ finito, $f : A \to A$ tiene inversa si y solo si $f$ es 1-1.

*Demostración.* (Directa)
($\Rightarrow$) Sea $A$ finito y suponga que $f : A \to A$ tiene inversa. Esto dice que cada elemento en el codominio tiene un elemento correspondiente en el domino, por lo tanto es sobre, y por lema anterior, es $1-1$.
($\Leftarrow$) Sea $A$ finito y suponga que $f : A \to A$ es $1-1$, entonces por lema anterior, $f$ es sobre. Considere $f^{-1} : A \to A$ como $f$ es función sobre, cada elemento en el dominio de $f^{-1}$ tiene solo un elemento correspondiente en su codominio, así que $f^{-1}$ es función sobre y, por lema, 1-1. Por lo tanto, $f$ tiene inversa. □

# 3. Trabajo Realizado

## 3.1. Polinomio de Permutación

Sabemos que una involución es una permutación que es su propia inversa, por ende, antes de probar que nuestro binomio es involución en $\mathbb{F}_q$, debemos primero probar que produce una permutación de $\mathbb{F}_q$. La prueba que proveemos es una generalización de la prueba encontrada en [5] que caracteriza las permutaciones del binomio $x(x^{\frac{q-1}{2}} + a)$, un caso particular de nuestro binomio donde $m = 1$.

**Proposición 3.1.1.** Sea $dmc(m, q-1) = 1$. $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ es un polinomio de permutación en $\mathbb{F}_q$ si y solo si $\eta(a^2 - 1) = 1$.

*Demostración.* (Contrapositivo)
($\Leftarrow$) Suponga que $P(x)$ no es polinomio de permutación, entonces $P(x)$ no es $1-1$.
**caso 1**: $f(c) = f(0) = 0$ para $c \in \mathbb{F}_q^*$
$\Rightarrow \mathrm{c}^m(c^{\frac{q-1}{2}} + a) = 0$
$\Rightarrow \mathrm{c}^{\frac{q-1}{2}} + a = 0$
$\Rightarrow$ a = -c$^{\frac{q-1}{2}}$
$\Rightarrow \eta(a^2 - 1) = \eta(-c^{\frac{q-1}{2}} - 1) = \eta(1 - 1) = \eta(0) = 0$
**caso 2**: $f(b) = f(c) \neq 0$ para $c, b \in \mathbb{F}_q^*$ y $b \neq c$
$\Rightarrow \mathrm{c}^m(c^{\frac{q-1}{2}} + a) = b^m(b^{\frac{q-1}{2}} + a)$
$\Rightarrow \mathrm{c}^m b^{-m} = (b^{\frac{q-1}{2}} + a)(c^{\frac{q-1}{2}} + a)^{-1}$
$\Rightarrow (\mathrm{cb}^{-1})^m = (b^{\frac{q-1}{2}} + a)(c^{\frac{q-1}{2}} + a)^{-1}$
Suponga que $\eta(c) = \eta(b)$
**caso 2.1**: $\eta(c) = \eta(b) = 1$
Sea $\alpha$ raíz primitva de $\mathbb{F}_q$
$\Rightarrow$c=$\alpha^{2k}$ y $b = \alpha^{2l}$ con $k, l \in \mathbb{Z}$
$\Rightarrow \mathrm{c}^{\frac{q-1}{2}} = (\alpha^{2k})^{\frac{q-1}{2}} = 1$ y $b^{\frac{q-1}{2}} = (\alpha^{2l})^{\frac{q-1}{2}} = 1$
$\Rightarrow \mathrm{c}^{\frac{q-1}{2}} = b^{\frac{q-1}{2}}$
**caso 2.2**: $\eta(c) = \eta(b) = -1$
$\Rightarrow$c=$\alpha^{2k+1}$ y $b = \alpha^{2l+1}$ con $k, l \in \mathbb{Z}$
$\Rightarrow \mathrm{c}^{\frac{q-1}{2}} = (\alpha^{2k+1})^{\frac{q-1}{2}} = -1$ y $b^{\frac{q-1}{2}} = (\alpha^{2l+1})^{\frac{q-1}{2}} = -1$
$\Rightarrow \mathrm{c}^{\frac{q-1}{2}} = b^{\frac{q-1}{2}}$

En ambos casos tenemos que $c^{\frac{q-1}{2}} = b^{\frac{q-1}{2}}$, entonces $c = b$, pero esto es una contradicción. Por lo tanto, $\eta(c) \neq \eta(b)$. Sin perder generalidad, podemos decir que $\eta(c) = 1$ y $\eta(b) = -1$. Entonces $c = \alpha^{2k}$ y $b = \alpha^{2l+1}$, $k, l \in \mathbb{Z}$

$\Rightarrow$ c$^{\frac{q-1}{2}} = 1$ y $b^{\frac{q-1}{2}} = -1$
$\Rightarrow \eta(cb) = \eta(\alpha^{2k+2l+1}) = \eta(\alpha^{2(k+l)+1}) = -1$
Por lema sabemos que $\eta(cb) = \eta(cb^{-1})$ y, como $m$ es impar, tenemos que
$\eta(cb^{-1}) = \eta((cb^{-1})^m) = -1$
$\Rightarrow \eta((b^{\frac{q-1}{2}} + a)(c^{\frac{q-1}{2}} + a)^{-1}) = \eta((b^{\frac{q-1}{2}} + a)(c^{\frac{q-1}{2}} + a)) = \eta((a-1)(a+1)) = \eta(a^2-1) = -1$
Por lo tanto, si $P(x)$ no es $1-1$, entonces $\eta(a^2-1) \neq 1$.

($\Rightarrow$) Suponga que $\eta(a^2-1) \neq 1$. Entonces tenemos dos casos, $\eta(a^2-1) = 0$ o $\eta(a^2-1) = -1$.
**caso 1**: $\eta(a^2-1) = 0$
Sea $\eta(a^2-1) = 0$, entonces $a^2 - 1 = 0$
$a^2 - 1 = 0 \Rightarrow$ a= $\pm 1$
Sabemos que $\forall\ d \in \mathbb{F}_q^*$, $d^{\frac{q-1}{2}} = \pm 1$. Por lo tanto, existe $c \in \mathbb{F}_q^*$ tal que $c^{\frac{q-1}{2}}$ sea el opuesto de $a$. Es decir,
$c^{\frac{q-1}{2}} = -a \Rightarrow$ c$^{\frac{q-1}{2}} + a = 0 \Rightarrow$ c$^m(c^{\frac{q-1}{2}} + a) = 0 \Rightarrow$ f(c)=f(0)
**caso 2** : $\eta(a^2-1) = -1$
Escoga $b = (a+1)^{m^{-1}}(a-1)^{-m^{-1}}$, por lema sabemos que $b \in \mathbb{F}_q^*$. Ahora, note que
$\eta(b) = \eta((a+1)^{m^{-1}}(a-1)^{-m^{-1}})$
$= \eta((a+1)^m(a-1)^{-m})$
$= \eta(((a+1)(a-1)^{-1})^m)$
$= \eta(((a+1)(a-1))^m)$
$= \eta((a+1)(a-1))$
$= \eta(a^2-1) = -1$
$\Rightarrow$ b$^{\frac{q-1}{2}} = -1$
$\Rightarrow$ P(b)=b$^m(b^{\frac{q-1}{2}} + a) = b^m(a-1)$
$= ((a+1)^{m^{-1}}(a-1)^{-m^{-1}})^m(a-1)$
$= (a+1)^{m^{-1}m}(a-1)^{-m^{-1}m}(a-1)$
$= (a+1)(a-1)^{-1}(a-1)$
$= a + 1 = P(1)$
Pero $b \neq 1$, por lo tanto, $P(x)$ no es $1-1$.
En ambos casos, tenemos que $P(x)$ no es polinomio de permutación. □

Es importante notar que para esta prueba hemos puesto una restricción en la $m$ tal que $dmc(m, q-1) = 1$. En [4] se provee una prueba que caracteriza todas las permutaciones de nuestro binomio $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ en $\mathbb{F}_q$. En el teorema del Dr. Daqin, se postula que todas las permutaciones de $P(x)$ tienen $dmc(m, q-1) \in \{1, 2\}$, es decir que no existen permutaciones de nuestro binomio con $dmc(m, q-1) > 2$. Incluso postula que para las permutaciones con $dmc(m, q-1) = 2$, solamente las $q = 4k+3$ permutan. Para nosotros esto significa que no hemos considerado todas las permutaciones de $\mathbb{F}_q$, y por lo tanto nos falta estudiarlas.

**Teorema 1.** (Wan Daqin) Sea $q$ impar y $P(x) = x^{m+\frac{q-1}{2}} + ax^m \in \mathbb{F}_q$, donde $m$ es un entero distinto de cero fijo. Entonces,

1. Sea $dmc(m, q-1) = 1$. Entonces $P(x)$ es un polinomio de permutación de $\mathbb{F}_q$ si y solo si $\eta(a^2-1) = 1$.

2. Sea $dmc(m, q-1) = 2$. Entonces $P(x)$ es un polinomio de permutación de $\mathbb{F}_q$ si y solo si $q = 4k+3$ y $\eta(a^2-1) = -1$.

3. Sea $dmc(m, q-1) > 2$. Entonces $P(x)$ no es un polinomio de permutación de $\mathbb{F}_q$.

## 3.2. Binomio de Involución

En [6], prueban que las inversas de $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ son de la forma $Q(x) = x^{m^{-1}+\frac{q-1}{2}} + bx^{m^{-1}} = x^{m^{-1}}(x^{\frac{q-1}{2}}+b)$ donde $m^{-1}$ es reducido (mód $\frac{q-1}{2}$), y dan fórmulas explícitas para calcular $b$. Se cree que aquí se encontraran condiciones iguales o adicionales que sean suficientes y necesarias para que nuestro binomio sea involución en $\mathbb{F}_q$. Con el corolario 2.2 de [6] pudimos reafirmar el próximo lema, que aunque ya estaba probado, nos ayuda a entender mejor cómo se comporta $P(x)$.

**Lema 3.2.1.** Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$

*Demostración.* (Directa)
Suponga que $P(x)$ es involución en $\mathbb{F}_q$.

$$P(\alpha^i) = \alpha^{im}(\alpha^{\frac{p-1}{2}i} + a) = \alpha^{im}((-1)^i + a)$$

$$P(P(\alpha^i)) = \alpha^{im^2}((-1)^i + a)^m(\alpha^{im\frac{q-1}{2}}((-1)^i + a)^{\frac{q-1}{2}} + a)$$

$$\alpha^i = \alpha^{im^2}((-1)^i + a)^m((-1)^{im}((-1)^i + a)^{\frac{q-1}{2}} + a)$$

$$\alpha^{i(1-m^2)} = ((-1)^i + a)^m((-1)^{im}((-1)^i + a)^{\frac{q-1}{2}} + a)$$

Note que $((-1)^i + a)^m((-1)^{im}((-1)^i + a)^{\frac{q-1}{2}} + a)$ es fijo para $i$ par o $i$ impar. Entonces existen $i, j$ con $i > j$ tal que $\alpha^{i(1-m^2)} = \alpha^{j(1-m^2)}$ con $i \equiv j \ (mod \ 2)$
$\Rightarrow \ \alpha^{(1-m^2)(i-j)} = 1$
$\Rightarrow \ (q-1)|(1-m^2)(i-j)$
$\Rightarrow \ (q-1)k = (1-m^2)(i-j)$, $k \in \mathbb{Z}$
Note que $i - j = 2l$, para $l \in \{1, 2, 3, \cdots, \frac{q-1}{2}\}$
$\Rightarrow \frac{q-1}{2}k = (1-m^2)l$
$\Rightarrow \frac{q-1}{2}|(1-m^2)l$
Considere $l = \frac{q-1}{2} - 1$. Note que $dmc(\frac{q-1}{2}, \frac{q-1}{2} - 1) = 1$, por lo tanto, $\frac{q-1}{2}|(1-m^2)$
$\Rightarrow m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ □

Como se mencionó al principio, el primer binomio de involución que exploramos fue el binomio de Cáceres y Colón $P_1(x) = x^{\frac{q-3}{2}}(x^{\frac{q-1}{2}} + a)$ que es un caso particular de nuestro binomio $P(x) = x^m(x^{\frac{q-1}{2}}+a)$ donde $m = \frac{q-3}{2}$. Las condiciones suficientes y necesarias para que $P_1(x)$ sea involución en $\mathbb{F}_q$ dependen de la reciprocidad de $a^2-1$. Queremos encontrar condiciones similares para nuestro binomio.

### 3.2.1. Binomio de Cáceres y Colón

**Lema 3.2.2.** Sea $i$ par, $P(x) = x^{\frac{q-3}{2}}(x^{\frac{q-1}{2}}+a)$, $a \neq 0$ es involución en $\mathbb{F}_q$ si y solo si $(a+1)^{\frac{q-1}{2}} = 1$

*Demostración.* (Directa)
($\Rightarrow$) Sea $\alpha$ raíz primitiva en $\mathbb{F}_q$ e $i$ par. Suponga que $P(x) = x^{q-2} + ax^{\frac{q-3}{2}}$, $a \neq 0$ involución en $\mathbb{F}_q$.

$$
\begin{aligned}
P(x) &= x^{q-2} + ax^{\frac{q-3}{2}} = x^{\frac{q-3}{2}}[x^{\frac{q-1}{2}} + a] = x^{\frac{q-1}{2}}x^{-1}[x^{\frac{q-1}{2}} + a] \\
P(\alpha^i) &= (\alpha^{\frac{q-1}{2}})^i(\alpha^i)^{-1}[(\alpha^{\frac{q-1}{2}})^i + a] = \alpha^{-i}[a+1] \\
P(P(\alpha^i)) &= (\alpha^{\frac{q-1}{2}})^{-i}(a+1)^{\frac{q-1}{2}}(\alpha^i)(a+1)^{-1}[(\alpha^{\frac{q-1}{2}})^{-i}(a+1)^{\frac{q-1}{2}} + a] \\
\alpha^i &= \alpha^i(a+1)^{\frac{q-1}{2}}(a+1)^{-1}[(a+1)^{\frac{q-1}{2}} + a] \\
1 &= (a+1)^{\frac{q-1}{2}}(a+1)^{-1}[(a+1)^{\frac{q-1}{2}} + a] \\
(a+1) &= (a+1)^{\frac{q-1}{2}}[(a+1)^{\frac{q-1}{2}} + a] \\
a+1 &= 1 + (a+1)^{\frac{q-1}{2}}a \\
a &= a(a+1)^{\frac{q-1}{2}} \\
1 &= (a+1)^{\frac{q-1}{2}}
\end{aligned}
$$

($\Leftarrow$) Sea $\alpha$ raíz primitiva en $\mathbb{F}_q$ e $i$ par. Suponga que $(a+1)^{\frac{q-1}{2}} = 1$, entonces tenemos que

$$
\begin{aligned}
P(x) &= x^{\frac{q-1}{2}}x^{-1}[x^{\frac{q-1}{2}} + a] \\
P(\alpha^i) &= (\alpha^i)^{\frac{q-1}{2}}(\alpha^i)^{-1}[(\alpha^i)^{\frac{q-1}{2}} + a] \\
&= (-1)^i(\alpha^{-i})[(-1)^i + a] \\
P(\alpha^i) &= \alpha^{-i}(a+1) \\
P(P(\alpha^i)) &= (\alpha^{-i})^{\frac{q-1}{2}}(a+1)^{\frac{q-1}{2}}(\alpha^i)(a+1)^{-1}[(\alpha^{-1})^{\frac{q-1}{2}}(a+1)^{\frac{q-1}{2}} + a] \\
&= (-1)^{-i}(1)(\alpha^i)(a+1)^{-1}[(-1)^{-i}(1) + a] \\
&= \alpha^i(a+1)^{-1}(a+1)^1 \\
P(P(\alpha^i)) &= \alpha^i
\end{aligned}
$$

Por definición de involución, $P(x)$ es involución en $\mathbb{F}_q$ □

**Proposición 3.2.1.** El binomio $P(x) = x^{q-2} + ax^{\frac{q-3}{2}}$, $a \neq 0$, es involución en $\mathbb{F}_q$ si y solo si

1. $q = 4k+1$ y $(a+1)^{\frac{q-1}{2}} = (a-1)^{\frac{q-1}{2}} = 1$
2. $q = 4k+3$, $(a+1)^{\frac{q-1}{2}} = 1$ y $(a-1)^{\frac{q-1}{2}} = -1$

*Demostración.* (Directa)
($\Rightarrow$) Sea $P(x) = x^{q-2} + ax^{\frac{q-3}{2}}$, $a \neq 0$ involución en $\mathbb{F}_q$. Como $\mathbb{F}_q$ es cuerpo, $q = p^r$ para $p$ primo, $p \neq 2$. Entonces $q$ es de la forma $q = 4k+1$ o $q = 4k+3$. Esto se puede dividir en dos casos, para $i$ par y para $i$ impar. En el caso de que $i$ sea par, por Lema 3.2.2, $(a+1)^{\frac{q-1}{2}} = 1$. En el caso de que $i$ sea impar y $q = 4k+1$, note que $\frac{q-3}{2} = \frac{4k+1-3}{2} = \frac{4k-2}{2} = \frac{2(2k-1)}{2} = 2k-1$. Por el Teorema 1 [4] sabemos que para que $P(x)$ sea permutación en $\mathbb{F}_q$, el $dmc(\frac{q-3}{2}, q-1) \in \{1, 2\}$. Al $\frac{q-3}{2}$ ser impar y $q-1$, par, tenemos que $dmc(\frac{q-3}{2}, q-1) = 1$, por lo tanto $\eta(a^2-1)$ tiene que ser 1. Esto nos dice que $\eta((a+1)(a-1)) = 1$. Como $(a+1)^{\frac{q-1}{2}} = \eta(a+1) = 1$, tenemos que $\eta(a-1) = (a-1)^{\frac{q-1}{2}} = 1$. Ahora, para el caso $q = 4k+3$ e $i$ impar, note que $\frac{q-3}{2} = \frac{4k+3-3}{2} = \frac{4k}{2} = 2k$. Por el Teorema 1 [4], esto nos dice que el $dmc(\frac{q-3}{2}, q-1) = 2$ y que $\eta(a^2-1)$ tiene que ser $-1$, es decir $\eta((a+1)(a-1)) = -1$. Como $\eta(a+1) = 1$ por Lema 2.2.4, esto implica que $(a-1)^{\frac{q-1}{2}} = -1$.

($\Leftarrow$) Sea $\alpha$ raíz primitiva de $\mathbb{F}_q$. Suponga que para $q = 4k+1$, $(a+1)^{\frac{q-1}{2}} = (a-1)^{\frac{q-1}{2}} = 1$ y que para $q = 4k+3$, $(a+1)^{\frac{q-1}{2}} = 1$ y $(a-1)^{\frac{q-1}{2}} = -1$. Sabemos que se puede dividir en dos casos, cuando $i$ es par y cuando $i$ es impar. En el caso $i$ par, por Lema 3.2.2, $(a+1)^{\frac{q-1}{2}} = 1$. En el caso $i$ impar, tenemos que:

$$\begin{aligned}
P(x) &= x^{\frac{q-3}{2}}[x^{\frac{q-1}{2}} + a] \\
P(x) &= x^{\frac{q-1}{2}}x^{-1}[x^{\frac{q-1}{2}} + a] \\
P(\alpha^i) &= (\alpha^{\frac{q-1}{2}})^i(\alpha^{-i})[(\alpha^{\frac{q-1}{2}})^i + a] \\
P(\alpha^i) &= (-1)^i(\alpha^{-i})[(-1)^i + a] \\
P(P(\alpha^i)) &= (-1)^{\frac{q-3}{2}i}(\alpha^{-i})^{\frac{q-3}{2}}[(-1)^i + a]^{\frac{q-3}{2}}[(-1)^{\frac{q-1}{2}i}(\alpha^{\frac{q-1}{2}})^{-i}[(-1)^i + a]^{\frac{q-1}{2}} + a] \\
&= (-1)^{\frac{q-3}{2}}(\alpha^{-i})^{\frac{q-3}{2}}(a-1)^{\frac{q-3}{2}}[(-1)^{\frac{q-1}{2}}(-1)(a-1)^{\frac{q-1}{2}} + a] \\
&= (-1)^{\frac{q-3}{2}}(-1)(\alpha^i)(a-1)^{\frac{q-3}{2}}[(-1)^{\frac{q+1}{2}}(a-1)^{\frac{q-1}{2}} + a] \\
P(P(\alpha^i)) &= (-1)^{\frac{q-1}{2}}(\alpha^i)(a-1)^{\frac{q-1}{2}}(a-1)^{-1}[(-1)^{\frac{q+1}{2}}(a-1)^{\frac{q-1}{2}} + a]
\end{aligned}$$

**caso 1:** $q = 4k+1$ y $(a+1)^{\frac{q-1}{2}} = (a-1)^{\frac{q-1}{2}} = 1$

$$\begin{aligned}
P(P(\alpha^i)) &= (\alpha^i)(a-1)^{-1}[(-1) + a] \\
P(P(\alpha^i)) &= \alpha^i
\end{aligned}$$

**caso 2:** $q = 4k+3$, $(a+1)^{\frac{q-1}{2}} = 1$ y $(a-1)^{\frac{q-1}{2}} = -1$

$$\begin{aligned}
P(P(\alpha^i)) &= (-1)(\alpha^i)(-1)(a-1)^{-1}[(-1) + a] \\
P(P(\alpha^i)) &= \alpha^i
\end{aligned}$$

□

Note que para el caso $q = 4k+3$, $k \in \mathbb{Z}$, el binomio de Cáceres y Colón tiene $m = \frac{q-3}{2} = \frac{4k}{2} = 2k$ y $m$ sería par, por el cual cae bajo el caso del $dmc(m, q-1) = 2$.

### 3.2.2. Involuciones con $dmc(m, q-1) = 1$

**Lema 3.2.3.** Sea $q = 4k+3$, $k \in \mathbb{Z}$ y $m$ impar. Si $\frac{q-1}{2}h = m^2 - 1$, entonces $h$ es par.

*Demostración.* Sea $q = 4k+3$, $k \in \mathbb{Z}$ y $m$ impar. Suponga que $\frac{q-1}{2}h = m^2 - 1$. Note que $\frac{q-1}{2} = \frac{4k+2}{2} = 2k+1$ es impar. Como $m$ es impar, $m^2 - 1$ es par. Ambos lados deben ser congruentes módulo 2, como $m^2 - 1$ es par, $\frac{q-1}{2}h$ tiene que ser par, por lo tanto $h$ es par. □

**Proposición 3.2.2.** Sea $dmc(m, q-1) = 1$ y $q = 4k+3$, $k \in \mathbb{Z}$. Si $\eta(a^2-1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{m+1} = (a-1)^{m+1} = 1$ y $(a+1)^{\frac{q-1}{2}} = 1$, entonces $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$.

*Demostración.* Sea $dmc(m, q-1) = 1$ y $q = 4k+3$ y $\alpha$ raíz primitiva en $\mathbb{F}_q$. Suponga que $\eta(a^2-1) = 1$, $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$, $(a-1)^{m+1} = (a-1)^{m+1} = 1$, y $(a+1)^{\frac{q-1}{2}} = 1$. Note que $m^2 = \frac{q-1}{2}h + 1$, $h \in \mathbb{Z}$. Entonces tenemos que

$$P(x) = x^m(x^{\frac{q-2}{2}} + a)$$
$$P(\alpha^i) = \alpha^{im}(\alpha^{\frac{q-1}{2}i} + a)$$
$$P(\alpha^i) = \alpha^{im}((-1)^i + a)$$
$$P(P(\alpha^i)) = \alpha^{im^2}((-1)^i + a)^m[\alpha^{\frac{q-1}{2}im}((-1)^i + a)^{\frac{q-1}{2}} + a]$$
$$P(P(\alpha^i)) = \alpha^{im^2}((-1)^i + a)^m[(-1)^i((-1)^i + a)^{\frac{q-1}{2}} + a]$$

Podemos dividir la ecuación en dos casos, $i$ par, e $i$ impar.
**caso $i$ par**:

$$\begin{aligned} P(P(\alpha^i)) &= \alpha^{im^2}(1 + a)^m[(1 + a)^{\frac{q-1}{2}} + a] \\ &= \alpha^{(\frac{q-1}{2}h+1)i}(1 + a)^m(1 + a) \\ &= \alpha^{i(\frac{q-1}{2}h)}\alpha^i(1 + a)^{m+1} \end{aligned}$$
$$P(P(\alpha^i)) = \alpha^i$$

**caso $i$ impar**:

$$\begin{aligned} P(P(\alpha^i)) &= \alpha^{im^2}(a - 1)^m[-(a - 1)^{\frac{q-1}{2}} + a] \\ &= \alpha^{i(\frac{q-1}{2}h+1)}(a - 1)^m(a - 1) \\ &= \alpha^{i(\frac{q-1}{2}h)}\alpha^i(a - 1)^{m+1} \\ &= (-1)^h\alpha^i \end{aligned}$$
$$P(P(\alpha^i)) = \alpha^i$$

En ambos casos tenemos que $P(P(\alpha^i)) = \alpha^i$ y por definición, $P(x)$ es involución en $\mathbb{F}_q$. □

### 3.2.3. Involuciones con $dmc(m, q-1) = 2$

**Lema 3.2.4.** Sea $q = 4k + 3$, $k \in \mathbb{Z}$ y $m$ par. Si $\frac{q-1}{2}h = m^2 - 1$, entonces $h$ es impar.

*Demostración.* Sea $q = 4k + 3$, $k \in \mathbb{Z}$ y $m$ par. Suponga que $\frac{q-1}{2}h = m^2 - 1$. Note que $\frac{q-1}{2} = \frac{4k+2}{2} = 2k + 1$ es impar. Como $m$ es par, $m^2 - 1$ es impar. Ambos lados deben ser congruentes módulo 2, como $m^2 - 1$ es impar, $\frac{q-1}{2}h$ tiene que ser impar, por lo tanto $h$ es impar. □

**Proposición 3.2.3.** Sea $dmc(m, q-1) = 2$ y $q = 4k + 3$, $k \in \mathbb{Z}$. Si $\eta(a^2 - 1) = -1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a + 1)^{m+1} = (a + 1)^{\frac{q-1}{2}} = 1$ y $(a - 1)^{m+1} = -1$, entonces $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$.

*Demostración.* Sea $dmc(m, q-1) = 2$ y $\alpha$ raíz primitiva de $\mathbb{F}_q$. Suponga que $\eta(a^2 - 1) = -1$ y $(a + 1)^{\frac{q-1}{2}} = 1$, esto implica que $(a - 1)^{\frac{q-1}{2}} = -1$. Suponga incluso que $m^2 \equiv 1$ (mód $\frac{q-1}{2}$) y $(a + 1)^{m+1} = 1$ y $(a - 1)^{m+1} = -1$.

$$P(\alpha^i) = \alpha^{im}(\alpha^{i\frac{q-1}{2}} + a)$$
$$P(\alpha^i) = \alpha^{im}((-1)^i + a)$$
$$\begin{aligned} P(P(\alpha^i)) &= \alpha^{im^2}((-1)^i + a)^m[\alpha^{im\frac{q-1}{2}}((-1)^i + a)^{\frac{q-1}{2}} + a] \\ &= \alpha^{i(\frac{q-1}{2}h+1}((-1) + a)^m[(-1)^{im}((-1)^i + a)^{\frac{q-1}{2}} + a] \\ P(P(\alpha^i)) &= (-1)^{ih}\alpha^i((-1)^i + a)^m[((-1)^i + a)^{\frac{q-1}{2}} + a] \end{aligned}$$

**caso $i$ par**:

$$\begin{aligned} P(P(\alpha^i)) &= \alpha^i(1 + a)^m((1 + a)^{\frac{q-1}{2}} + a) \\ &= \alpha^i(1 + a)^m(1 + a) \\ &= \alpha^i(1 + a)^{m+1} \\ P(P(\alpha^i)) &= \alpha^i \end{aligned}$$

**caso $i$ impar**:

$$\begin{aligned} P(P(\alpha^i)) &= (-1)^h\alpha^i(a - 1)^m((a - 1)^{\frac{q-1}{2}} + a) \\ &= (-1)^h\alpha^i(a - 1)^m(a - 1) \\ &= (-1)^h\alpha^i(a - 1)^{m+1} \\ &= (-1)^{h+1}\alpha^i \\ P(P(\alpha^i)) &= \alpha^i \end{aligned}$$

En ambos casos tenemos que $P(P(\alpha^i)) = \alpha^i$ que por definición significa que $P(x)$ es involución en $\mathbb{F}_q$. □

## 3.3. Conjeturas

### 3.3.1. Conjeturas de Involuciones con $dmc(m, q-1) = 1$

Computacionalmente (ver Apéndice) se ha encontrado que las condiciones que hemos probado que son necesarias para que $P(x)$ sea involución, también son suficientes. La conjetura 2 es una reducción de la conjetura 1, es decir que al probar esta se puede probar la conjetura 1. Las conjeturas 3, 4, 5 también son reducciones de la 1. Probar cualquiera de ellas bastaría para probar la conjetura 1.
Es importante notar que la $i$ es la potencia de la raíz primitiva, es decir, si se dice que $i$ es par, entonces solo consideramos los elementos de $\mathbb{F}_q$ que sean potencias impares de $\alpha$. Lo mismo cuando $i$ es impar, se está hablando de las potencias pares de $\alpha$.

**Conjetura 1.** Sea $dmc(m, q-1) = 1$ y $q = 4k + 3$. Si $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $\eta(a^2 - 1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a + 1)^{m+1} = (a - 1)^{m+1} = 1$ y $(a + 1)^{\frac{q-1}{2}} = 1$.

**Conjetura 2.** Sea $dmc(m, q - 1) = 1$ e $i$ par. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a + 1)^{m+1} = 1$.

**Conjetura 3.** Sea $dmc(m, q - 1) = 1$ e $i$ par. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a + 1)^{\frac{q-1}{2}} = 1$.

**Conjetura 4.** Sea $dmc(m, q-1) = 1$ e $i$ impar. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a-1)^{m+1} = 1$.

**Conjetura 5.** Sea $dmc(m, q-1) = 1$ e $i$ impar. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a-1)^{\frac{q-1}{2}} = 1$.

### 3.3.2. Conjeturas de Involuciones con $dmc(m, q-1) = 2$

Computacionalmente (ver Apéndice) se ha encontrado que las condiciones que hemos probado que son necesarias para que $P(x)$ sea involución, también son suficientes. Similar al caso de $dmc(m, q-1) = 1$, tenemos varias conjeturas (7, 8, 9, 10) que son reducciones de la conjetura que postula que las condiciones son suficientes para que $P(x)$ sea involución en $\mathbb{F}_q$ (conjetura 6). Probar cualquiera de ellas bastaría para probar la conjetura 6.
Similar a las conjeturas con $dmc(m, q-1) = 1$, cuando se habla de pa laridad de $i$, se está hablando de las potencias de $\alpha$ con la misma paridad.

**Conjetura 6.** Sea $dmc(m, q-1) = 2$ y $q = 4k+3$. Si $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $\eta(a^2-1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{m+1} = (a+1)^{\frac{q-1}{2}} = 1$ y $(a-1)^{m+1} = -1$.

**Conjetura 7.** Sea $dmc(m, q-1) = 2$ e $i$ par. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a+1)^{m+1} = 1$.

**Conjetura 8.** Sea $dmc(m, q-1) = 2$ e $i$ par. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a+1)^{\frac{q-1}{2}} = 1$.

**Conjetura 9.** Sea $dmc(m, q-1) = 2$ e $i$ impar. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a-1)^{m+1} = -1$.

**Conjetura 10.** Sea $dmc(m, q-1) = 2$ e $i$ impar. Si $x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $(a-1)^{\frac{q-1}{2}} = -1$.

### 3.3.3. Conjeturas sobre la forma de $m$

Lo siguiente se encontró computacionalmente para $q \leq 569$.

**Conjetura 11.** Sea $q-1 = 2^e q_1^{e_1} \cdots q_r^{e_r}$, $d = 2^f q_1^{k_1} \cdots q_r^{k_r}$. Si $P(x) = x^m(x^{\frac{q-1}{2}} + a)$ es involución en $\mathbb{F}_q$, entonces $f \leq e$ y

$$m = \frac{q-1}{d}k - 1$$

donde $d+1$ es la cantidad de puntos fijos de $P(x)$.

Se verificó si las $k$ se podían escribir, al igual que para el caso de los monomios de involución, de las siguientes maneras

$$k = \begin{cases} 2(\frac{q-1}{d})^{\phi(d)-1} \\ (\frac{q-1}{2d})^{\phi(d)-1} + \frac{d}{2} \\ (\frac{q-1}{2d})^{\phi(\frac{d}{2})} + t, t \in \{0, \frac{d}{2}\} \end{cases}$$

reduciendo $k$ $(mod\ d)$. Sin embrago, hay algunas $k$ que no se pueden escribir de estas maneras.

*Contraejemplo.* Sea $P(x) = x^{34}(x^{21}+3)$ es involución en $\mathbb{F}_{43}$. Note que $m = 34 = \frac{q-1}{6}(5) - 1$ y $k = 5$, $k$ no se puede escribir de las formas dichas arriba.

Se fijó la cantidad de puntos fijos $d+1$ de las involuciones. Se consideran los casos $d = 4, 6, 8$.

### 3.3.4. Involuciones con $d = 2$

Al fijar $d = 2$, se encontró computacionalmente que

$$m = \begin{cases} (\frac{q-1}{2})1 - 1 \\ (\frac{q-1}{2})2 - 1 \end{cases}$$

donde $q - 1 = 2^e q_1^{k_1} \cdots q_n^{k_n}$.

**Conjetura 12.** Sea $q - 1 = 2^e q_1^{e_1} \cdots q_r^{e_r}$, $d = 2$. $P(x)$ es involución en $\mathbb{F}_q$ solo si

$$m = (\frac{q-1}{2})k - 1$$

donde

$$k = (\frac{q-1}{d})^{\phi(d)} + t,\ t \in \{0, \frac{d}{2}\}$$

$k$ es reducido *mod* $d$.

Es importante notar que en este caso $\phi(2) = 1 = \phi(1)$. Es decir $\phi(d) = \phi(d/2)$.

### 3.3.5. Involuciones con $d = 4$

Al fijar $d = 4$, se encontró computacionalmente que

$$m = \begin{cases} (\frac{q-1}{4})1 - 1 \\ (\frac{q-1}{4})2 - 1 \\ (\frac{q-1}{4})3 - 1 \\ (\frac{q-1}{4})4 - 1 \end{cases}$$

donde $q - 1 = 2^e q_1^{k_1} \cdots q_n^{k_n}$

**Conjetura 13.** Sea $q - 1 = 2^e q_1^{e_1} \cdots q_r^{e_r}$, $k_1 = 1, 3$, $k_2 = 2, 4$ y $d = 2^2$. $P(x)$ es involución en $\mathbb{F}_q$ solo si

$$m = \begin{cases} (\frac{q-1}{4})k_1 - 1 \\ (\frac{q-1}{4})k_2 - 1 \end{cases}$$

donde

$$k_1 = (\frac{q-1}{2d})^{\phi(\frac{d}{2})-1} + t,\ t \in \{0, \frac{d}{2}\}$$

$$k_2 = 2(\frac{q-1}{d})^{\phi(\frac{d}{2})-1} + t,\ t \in \{0, \frac{d}{2}\}$$

$k$ es reducido *mod* $d$.

### 3.3.6. Involuciones con $d = 6$

Al fijar $d = 6$, se encontró que

$$m = \begin{cases} (\frac{q-1}{6})1 - 1 \\ (\frac{q-1}{6})2 - 1 \\ (\frac{q-1}{6})4 - 1 \\ (\frac{q-1}{6})5 - 1 \end{cases}$$

donde $q - 1 = 2^e q_1^{k_1} \cdots q_n^{k_n}$, con $e \geq 1$.

**Conjetura 14.** Sea $q - 1 = 2^e q_1^{e_1} \cdots q_r^{e_r}$, $d = 6$, y $k = 1, 4$. $P(x)$ es involución en $\mathbb{F}_q$ solo si

$$m = (\frac{q-1}{6})k - 1, \ e \geq 1$$

donde

$$k = (\frac{q-1}{d})^{\phi(\frac{d}{2})} + t, t \in \{0, \frac{d}{2}\}$$

$k$ es reducido *mod* $d$.

**Conjetura 15.** Sea $q - 1 = 2^e q_1^{e_1} \cdots q_r^{e_r}$, $d = 6$, y $k = 2, 5$. $P(x)$ es involución en $\mathbb{F}_q$ solo si

$$m = (\frac{q-1}{6})k - 1, \ e \geq 1$$

donde

$$k = 2(\frac{q-1}{d})^{\phi(\frac{d}{2})-1} + t, t \in \{0, \frac{d}{2}\}$$

$k$ es reducido *mod* $d$.

Para una misma $q$, pueden haber dos $k$, $1, 5$ o $2, 4$, o solamente una $k$ $2, 4, 5$.

### 3.3.7. Involuciones con $d = 8$

Al fijar $d = 8$, se encontró que

$$m = \begin{cases} (\frac{q-1}{4})h_1 - 1, q - 1 = 2^3 q_1^{k_1} \cdots q_r^{k_r} \\ (\frac{q-1}{4})h_2 - 1, q - 1 = 2^4 q_1^{k_1} \cdots q_r^{k_r} \end{cases}$$

donde $h_1 = 2, 6$ y $h_2 = 1, 3, 5, 7$.

**Conjetura 16.** Sea $q - 1 = 2^e q_1^{e_1} \cdots q_r^{e_r}$, y $d = 2^3 = 8$. $P(x)$ es involución en $\mathbb{F}_q$ solo si

$$m = \begin{cases} (\frac{q-1}{8})k_1 - 1, & e = 3 \\ (\frac{q-1}{8})k_2 - 1, & e = 4 \end{cases}$$

donde $k_1 = 2, 6$ y $k_2 = 1, 3, 5, 7$.

### 3.4. Proposiciones Falsas

Al momento de construir nuestro binomio pensamos que es un paso razonable es combinar monomios de involución para crear un binomio de involución, de lo cual surgieron naturalmente algunas preguntas postuladas abajo. Se incluyen también proposiciones falsas que hemos encontrado a lo largo de la investigación.

**Proposición 3.4.1.** Si $x^m(x^{\frac{q-1}{2}}+a)$ es involución en $\mathbb{F}_q$, entonces $x^m$ es involución en $\mathbb{F}_q$.

*Contraejemplo.* Sea $m=11$, $a=3$, entonces se puede verificar que $P(x)=x^{11}(x^8+3)$ es involución en $\mathbb{F}_{17}$, pero $x^{11}$ no es involución en $\mathbb{F}_{17}$.

**Proposición 3.4.2.** Si $x^m$ es involución en $\mathbb{F}_q$, entonces $x^m(x^{\frac{q-1}{2}}+a)$ es involución en $\mathbb{F}_q$.

*Contraejemplo.* Sea $m=7$, entonces se puede verificar que $P(x)=x^7$ es involución en $\mathbb{F}_{17}$, pero $P(x)=x^m(x^{\frac{q-1}{2}}+a)$ no es involución en $\mathbb{F}_q$.

**Proposición 3.4.3.** Si $P(x)=x^m(x^{\frac{q-1}{2}}+a)$ es involución en $\mathbb{F}_q$, entonces $m^2\equiv 1\ mod\ (q-1)$

*Contraejemplo.* Sea $q=113$, $a=27$, $m=27$, note que $P(x)=x^{27}(x^{56}+27)$ es involución en $\mathbb{F}_{113}$ pero $m^21\ mod\ (112)$

**Proposición 3.4.4.** Si $m^2\equiv 1\ mod\ (q-1)$, entonces $P(x)=x^m(x^{\frac{q-1}{2}}+a)$ es involución en $\mathbb{F}_q$

*Contraejemplo.* Sea $q=113$, $a=27$, $m=1$, note que $m^2\equiv 1\ mod\ 112$ pero $P(x)=x^1(x^{56}+27)$ no es involución en $\mathbb{F}_{113}$.

## 4. Trabajo Futuro

- Encontrar condiciones que sean suficientes y necesarias para cuando $q=4k+1$ sea involución en $\mathbb{F}_q$.
- Probar conjeturas de condiciones suficientes para que $P(x)$ sea involución en $\mathbb{F}_q$ (conjeturas 1 y 6).
- Buscar fórmulas explícitas para la forma de $m$ parecidas a las de [2].
- Trabajar con el corolario 2.2 de [6] que provee una fórmula explícita para el binomio inverso de $P(x)$.

## 5. Presentaciones

Esta investigación fue presentada en el Seminario Interuniversitario de Investigación en Ciencias Matemáticas (SIDIM) que se llevó a cabo del 23 al 14 de marzo de 2018 con afiche y en el *Junior Technical Meeting* (JTM) y el *Puerto Rico Interdisciplinary Scientific Meeting* (PRISM) que se llevó a cabo el 28 de abril del 2018 con una presentación oral.

# 6. Bibliografía

## Referencias


[1] A. Cáceres and O. Colón-Reyes. Some Criteria for Permutation Binomials. (Sept):1–11, 1997.

[2] F. Castro, C. Corrada-Bravo, N. Pacheco-Tallaj, and I. Rubio. Explicit Formulas for Monomial Involutions over Finite Fields. 2015.

[3] C. Corrada and I. Rubio. Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials.

[4] W. Daqing. Permutation Binomials over Finite Fields. *Acta Mathematica Sinica, New Series*, 10(Special Issue (Jan.)):30–35, 1994.

[5] R. Lidl and H. Niederreiter. *Finite Fields*. Addison-Wesley, Cambridge, Massachusetts, 1983.

[6] Q. Wang. On inverse permutation polynomials. *Finite Fields and their Applications*, 15(2):207–213, 2009.


# 7. Apéndice

# Binomios de Involucion en F_p con dmc(m,q-1)=1

June 8, 2018

## 1 Lillian González Albino

### 1.1 Binomios de Involución con $dmc(m, q-1) = 1$

A continuación se encuentra el código utilizado para formar conjeturas postuladas en el technical report Enero 2018. Se documenta todo el procedimiento comenzando con las funciones que se utilizaron para probar que $P(x) = x^m(x^{\frac{p-1}{2}} + a)$ es permutación en $\mathbb{F}_q$, seguido por las conjeturas formadas para buscar condiciones suficientes y necesarias para que $P(x)$ sea involución en $\mathbb{F}_q$. Se documentan los resultados de las conjeturas, pero no se despliegan ya que los resultados contradicen las conjeturas, también se documenta los próximos pasos a seguir. Al final se despliegan los resultados de la última conjetura hecha ya que los resultados van acorde con la conjetura.

Verificar conjetura: Sea $dmc(m, q-1) = 1$. Si $\eta(a^2-1) = 1$, entonces $P(x) = x^m(x^{\frac{q-1}{2}}+a)$ es permutación en $\mathbb{F}_q$

In [2]:
```
#input: p primo
#output: lista de enteros
#recibe un primo p y devuelve una lista de todas las a que
#satisfacen que a^2-1 se un residuo cuadratico mod p

def findAs(p):
    listOfAs =[]
    b = quadratic_residues(p)
    for a in range(p):
        if((a^2-1)%p in b):
            if(a != 0 and (a^2-1)%p != 0):
                listOfAs.append(a)
    return listOfAs

#input: p primo
#output: lista de enteros
#recibe un primo p y devuelve una lista de todas las m
#que sean relativamente primas a p-1

def findMs(p):
    listOfMs = []
    for m in range(p):
        if(gcd(m,p-1)==1):
            listOfMs.append(m)
    return listOfMs

#input: primo p, int a, int m
#output: bool
#recibe un primo p, una a y una m y verifica si el polinomio
```

```
#con las dadas variables es de permutacion

def checkifPP(p,a,m):
    A = range(p)
    B = []
    for x in A:
        P = x^m * (x^((p-1)/2) + a)
        B.append(P%p)
    if(set(A) == set(B)):
        return True
    else:
        return False

#input: primo p, lista de enteros lA, lista de enteros lM
#output: void
#recibe un primo p y una lista de as y ms y verifica si todas
#las combinaciones de as y ms (bajo mod p) son polinomios de
#permutacion. Despliega las combinaciones (p,m,a) que no sean
#de permutacion

def checkAllPP(p, lA, lM):
    for a in lA:
        for m in lM:
            if(checkifPP(p,a,m)==False):
                print(p,a,m)
```

Funciones que devuelven todas las involuciones en $\mathbb{Z}_q$ dado un primo $q$.

In [3]:
```
#input: p pirmo, int c
#output: i int
#recibe un p primo y un int c, calcula alpha^i
#(alpha raiz primitiva de Z_p) y devuelve i

def findi(p, c):
    alpha = primitive_root(p)
    for i in range(p):
        if((alpha^i)%p == c):
            return i

#input: p primo, int m, int a
#output: bool
#recibe un p primo, int m, int a, y verifica si el binomio
#con las dadas variables es de involucion
#add verificar puntos fijos > 0

def checkifInv(p,m,a):
    h = (p-1)/2
    d = 0
    for x in range(1,p+1):
        Px = ( x^m * (x^h + a) )%p
        PPx = ( Px^m * (Px^h + a) )%p
        if(Px == x):
            d += 1
        if(PPx == 0):
            PPx = p
```

```
            if(PPx != x):
                return False
        if(d > 0):
            return True
        else:
            return False

#input: p primo
#output: lista (int, int, int)
#recibe un primo p y calcula todas las involucione de esa p
#y devuelve una lista con elementos tuplas (p,m,a) que hacen
#el binomio una involucion

def findAllInv(p):
    lM = findMs(p)
    lA = findAs(p)
    lInv = []
    for m in lM:
        for a in lA:
            if(checkifInv(p,m,a)):
                lInv.append((m,a))
    return lInv

#input: primo p, int m, int a
#output: int d
#recive un primo p, int m, int a, verifica si es un
#polinomio de involucion y si lo es devuelve la cantidad
#de puntos fijos del mismo

def countFixedPoints(p,m,a):
    if(checkifInv(p,m,a)==False):
        return -1
    else:
        d = 0
        for x in range(1,p):
            Px = ( x^m * (x^((p-1)/2) + a) )%p
            if( x == Px ):
                d += 1
        return d

#input: p primo, int m,a,d
#output: int k
#recibe p primo, int m,a,d y devuelve k = ((m+1)*d)/(p-1)
#note: solo funciona cuando las variables dadas son
#involucion del polinomio

def findK(p,m,a,d):
    k = ((m+1)*d)/(p-1)
    return k

#input: p primo
#output: lista (int,int,int,int)
#recibe un primo p, calcula todas las involuciones,
#sus puntos fijos, y su k = ((m+1)*d)/(p-1) y los
```

```
        #devuelve en una lista de tuplas conteniendo las invulociones

        def findAllKandD(p):
            lI = findAllInv(p)
            lInvDK = []
            for elem in lI:
                m = elem[0]
                a = elem[1]
                d = countFixedPoints(p,m,a)
                if( d != 0 ):
                    k = findK(p,m,a,d)
                    lInvDK.append((p,m,a,d,k))
            return lInvDK
```

Funcion que devuelve todas las involuciones de $\mathbb{Z}_q$ para distintos primos $q$

```
In [4]: #input: int frm, int n, int fixpoint (opcional)
        #output: void
        #verifica todas las involuciones desde el proximo primo despues de
        #frm y los proximos n primos despues de from y despliega las
        #combiaciones (p,m,a,d,k) de involuciones. Si el argumento fixpoint
        #esta dado, solo despliega las involvuciones con fixpoint cantidad
        #de puntos fijos (sin incluir el 0)

        def findInvolution(frm, n, fixpoint = None):
            P = Primes()
            p = frm -1
            for i in range(n):
                p = P.next(p)
                for elem in findAllKandD(p):
                    d = elem[3]
                    if(fixpoint is None):
                        print(elem)
                    else:
                        if(d == fixpoint):
                            print(elem)
```

```
In [5]: findInvolution(17, 1)
```

```
(17, 3, 3, 4, 1)
(17, 7, 3, 4, 2)
(17, 11, 3, 4, 3)
(17, 15, 3, 4, 4)
```

Función complementaria que devuelve todas las $i$ tal que $\alpha^i = c$ para una lista dada de c's ($\alpha$ raiz primitida de $\mathbb{Z}_q$)

```
In [5]: #input: p primo, lista int lC
        #output: void
        #recibe un primo p y una lista de cs, despliega todas las i tal
        #que alpha^i==c (alpha raiz primitida de Z_p)

        def findAlli(p, lC):
            for x in lC:
                print(x,findi(p, x))
```

Funciones complementaria que clasifica a $q$ de la forma $4k+1$ o $4k+3$ ($k \in \mathbb{Z}$)

```
In [6]: #input: p primo
        #output: 1,3
        #coge un primo p y devuelve 1 si p=4k+1 y, 3 si p=4k+3
        def findPform(p):
            pForm = 0
            if(((p-1) % 4) == 0):
                pForm = 1
            if(((p-3) % 4) == 0):
                pForm = 3
            return pForm

        #input: p primo
        #output: coge los primeros 10 primos desde p y
        #devuelve 1 si p=4k+1 y, 3 si p=4k+3 para cada p
        def pForms(startP):
            P = Primes()
            p = startP - 1
            for i in range(10):
                p = P.next(p)
                print(p, findPform(p))
```

Tratanto de probar conjeturas pasadas sobre $P(x)$ se encontró que para $m^2 = \frac{q-1}{2}(impar) + 1$ no se cumplen. Esta función es para encontrar $m^2$ que satisfacen estas condiciones para poder estudiarlas.

```
In [7]: #buscar involuciones
        #buscar m^2 que cumplan con condiciones dadas
        def m_squared(p):
            invs = findAllInv(p)
            for inv in invs:
                #print(inv)
                m = inv[0]
                a = inv[1]
                var = (2*(m^2-1))/(p-1)
                print(m,a,(m^2)%p,var)
```

Fijando diferentes $q$ se encontró con la función anterior que el único primo $q < 90$ que satisface las condiciones dadas es $q = 17$. Estudiaremos más a fondo este primo.

Función complementaria que verifica proposiciones (pasadas como parámetros) para diferentes primos $p$

```
In [8]: #input: p primo, int amount, funcion func (que su output sea void)
        #output: void
        #Despliega el output de la funcion (func) para una
        #cantidad (amount) de primos
        def checkpropDifferentP(p, amount, func):
            P = Primes()
            for i in range(amount):
                func(p)
                p = P.next(p)
```

Verificar conjetura 1: Sea $dmc(m, q-1) = 1$. Si $\eta(a^2-1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{m+1} = 1$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [9]: #input: p primo
        #output: void
        # verifica la conjetura: gcd(m,p-1)==1 y a^2-1 r.c. y
        #m^2 congr 1 (mod) (p-1)/2 y (a+1)^(m+1) % p == 1  => involucion
        def checkprop1(p):
            lA = findAs(p)
            for m in range(p):
                if(gcd(m, p-1)==1):
                    halfp = (p-1)/2
                    if(m^2 % halfp == 1):
                        for a in lA:
                            plusa = a+1
                            minusa = a-1
                            expo = m+1
                            if(plusa^expo % p == 1):
                                print(p,m,a,checkifInv(p,m,a))
```

Se encontró en el output anterior, salieron todas las involuciones, sin embargo, también salieron otras combinaciones de (p,m,a) que no hacen $P(x)$ una involución.

Verificar conjetura 2: Sea $q(m, q-1) = 1$. Si $\eta(a^2-1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{m+1} = 1$ y $(a-1)^{m+1} = 1$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [10]: #input: p primo
         #output: void
         # verifica la conjetura: gcd(m,p-1)==1 y a^2-1 r.c. y
         #m^2 congr 1 (mod) (p-1)/2 y (a+1)^(m+1) == 1  y
         #(a-1)^(m+1) == 1 => involucion
         def checkprop2(p):
             lA = findAs(p)
             for m in range(p):
                 if(gcd(m, p-1)==1):
                     halfp = (p-1)/2
                     if(m^2 % halfp == 1):
                         for a in lA:
                             plusa = a+1
                             minusa = a-1
                             expo = m+1
                             if(plusa^expo % p == 1):
                                 if(minusa^expo % p == 1):
                                     print(p,m,a,checkifInv(p,m,a))
```

Se encontró en el output anterior que, al igual que en la conjetura 1, salen "todas" las involuciones pero también salen otras combinaciones de (p,m,a) que no hacen a $P(x)$ una involución. Con la excepción del p=17 en el cual solo salen mitad de las permutaciones.

Observacion: Para todas las involuciones $(a+1)^{m+1} = 1$ pero para solo algunas $(a-1)^{m+1} = 1$.

Modificación conjetura 2: Sea $dmc(m, q-1) = 1$. Si $\eta(a^2-1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{m+1} = 1$ y $[(a-1)^{m+1} = 1$ o $(a-1)^{m+1} = -1]$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [11]: #input: p primo
         #output: void
         # verifica la conjetura: gcd(m,p-1)==1 y a^2-1 r.c. y
         #m^2 congr 1 (mod) (p-1)/2 y (a+1)^(m+1) == 1  y (a-1)^(m+1) == 1
         #o -1 => involucion
```

```
def checkprop25(p):
    lA = findAs(p)
    for m in range(p):
        if(gcd(m, p-1)==1):
            halfp = (p-1)/2
            if(m^2 % halfp == 1):
                for a in lA:
                    plusa = a+1
                    minusa = a-1
                    expo = m+1
                    if(plusa^expo % p == 1):
                        v = -1 % p
                        if(minusa^expo % p == 1):
                            print(p,m,a,checkifInv(p,m,a))
                        if(minusa^expo % p == v):
                            print(p,m,a,checkifInv(p,m,a))
```

Se encontró en el output anterior que con las condiciones dadas salen todas las involuciones (incluyendo p=17) pero también salen combinaciones (p,m,a) que no hacen a P(x) una involución

Próximo paso: verificar otras condiciones que pueden reducir el output para que solamente salgan las involuciones. Aparte, averiguar cuándo $(a-1)^{m+1}$ es igual a 1 y cuándo es igual a -1.

Verificar conjetura 3: Sea $dmc(m, q-1) = 1$. Si $\eta(a^2-1) = 1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{m+1} = 1$ y $(a+1)^{\frac{q-1}{2}} = 1$ y $[(a-1)^{m+1} = 1$ o $(a-1)^{m+1} = -1]$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [12]: #input: p primo
         #output: void
         # verifica la conjetura: gcd(m,p-1)==1 y a^2-1 r.c.
         #y m^2 congr 1 (mod) (p-1)/2 y (a+1)^(m+1) == 1  y (a-1)^(m+1) == 1
         #o -1 y (a+1)^((p-1)/2) => involucion
         def checkprop3(p):
             lA = findAs(p)
             for m in range(p):
                 if(gcd(m, p-1)==1):
                     halfp = (p-1)/2
                     if(m^2 % halfp == 1):
                         for a in lA:
                             plusa = a+1
                             minusa = a-1
                             expo = m+1
                             halfp = (p-1)/2
                             if(plusa^expo % p == 1):
                                 if(plusa^halfp % p == 1):
                                     v = -1 % p
                                     if(minusa^expo % p == 1):
                                         print(p,m,a,checkifInv(p,m,a))
                                     if(minusa^expo % p == v):
                                         print(p,m,a,checkifInv(p,m,a))
```

Se encontró en el output anterior que para $q = 4k+3$ salen todas las involuciones y no sobran ningunos pares ordenados (p,m,a) que no hagan a $P(x)$ involución. Es decir, tenemos condiciones suficientes y necesarias para que $P(x)$ sea involución. Sin embargo, para $q = 4k+1$, aunque salen todas las involcuiones todavía salen otros pares ordenados (p,m,a) que no hacen a $P(x)$ una involución.

Próximos pasos:

1) Ver si para $q = 4k+3$ se puede eliminar el caso de $(a-1)^{m+1} = -1$ y si con $(a-1)^{m+1} = 1$ junto con

las otras dos condiciones es suficiente y necesario para generar las involuciones.
2) Buscar otra condición adicional para $q = 4k + 1$ que haga que sean suficientes y necesarias para que sea involución.
3) (De las observaciones de la conjetura 2 modificada) Ver cuándo $(a-1)^{m+1} = -1$ y cuándo $(a-1)^{m+1} = 1$
Verificar conjetura 4: Sea $dmc(m, q-1) = 1$ y $q = 4k + 3$. Si $\eta(a^2 - 1) = 1$ y $m^2 \equiv 1\ (mod\ \frac{q-1}{2})$ y $(a + 1)^{m+1} = 1$ y $(a + 1)^{\frac{p-1}{2}} = 1$ y $(a - 1)^{m+1} = 1$, entonces P(x) es involución en $\mathbb{F}_q$
Todo reducido mod $q$

```
In [13]: #input: p primo
         #output: void
         # verifica la conjetura 2: p=4k+3 y gcd(m,p-1)==1 y a^2-1 r.c.
         #y m^2 congr 1 (mod) (p-1)/2 y (a+1)^(m+1) == 1  y (a-1)^(m+1) == 1
         #y (a+1)^((p-1)/2)=1 => involucion
         def checkprop4(p):
             if(findPform(p)==3):
                 lA = findAs(p)
                 for m in range(p):
                     if(gcd(m, p-1)==1):
                         halfp = (p-1)/2
                         if(m^2 % halfp == 1):
                             for a in lA:
                                 plusa = a+1
                                 minusa = a-1
                                 expo = m+1
                                 halfp = (p-1)/2
                                 if(plusa^expo % p == 1):
                                     if(plusa^halfp % p == 1):
                                         if(minusa^expo % p == 1):
                                             print(p,m,a,checkifInv(p,m,a))
             else:
                 print("p=4k+1")
```

Se encontró con la función anterior que las condiciones dadas son suficiente y necesarias para que $P(x)$ esa involución con $q = 4k + 3$
Próximos pasos:
1) Buscar otra condición adicional para $p = 4k + 1$ que haga que sean suficientes y necesarias para que sea involución.
2) (de las observaciones de la conjetura 2 modificada) Ver cuándo $(a-1)^{m+1} = -1$ y cuándo $(a-1)^{m+1} = 1$
Resultados de la conjetura 4

```
In [15]: #lista de primos de la forma p=4k+3
         p3 = [7,11,19,23,31,43,47,59,67,71,79,83]
         for p in p3:
             checkprop4(p)
```

```
(7, 5, 3, True)
(11, 9, 2, True)
(11, 9, 4, True)
(19, 17, 5, True)
(19, 17, 6, True)
(19, 17, 8, True)
(19, 17, 10, True)
(23, 21, 2, True)
(23, 21, 3, True)
(23, 21, 5, True)
```

```
(23, 21, 7, True)
(23, 21, 17, True)
(31, 19, 3, True)
(31, 29, 3, True)
(31, 29, 6, True)
(31, 29, 8, True)
(31, 29, 9, True)
(31, 29, 15, True)
(31, 29, 17, True)
(31, 29, 19, True)
(43, 41, 5, True)
(43, 41, 10, True)
(43, 41, 12, True)
(43, 41, 14, True)
(43, 41, 15, True)
(43, 41, 16, True)
(43, 41, 22, True)
(43, 41, 24, True)
(43, 41, 37, True)
(43, 41, 39, True)
(47, 45, 2, True)
(47, 45, 3, True)
(47, 45, 5, True)
(47, 45, 7, True)
(47, 45, 8, True)
(47, 45, 13, True)
(47, 45, 15, True)
(47, 45, 17, True)
(47, 45, 26, True)
(47, 45, 33, True)
(47, 45, 35, True)
(59, 57, 2, True)
(59, 57, 4, True)
(59, 57, 6, True)
(59, 57, 8, True)
(59, 57, 16, True)
(59, 57, 18, True)
(59, 57, 20, True)
(59, 57, 21, True)
(59, 57, 26, True)
(59, 57, 27, True)
(59, 57, 28, True)
(59, 57, 47, True)
(59, 57, 50, True)
(59, 57, 52, True)
(67, 43, 23, True)
(67, 43, 63, True)
(67, 65, 5, True)
(67, 65, 15, True)
(67, 65, 16, True)
(67, 65, 18, True)
(67, 65, 20, True)
(67, 65, 22, True)
(67, 65, 23, True)
```

```
(67, 65, 24, True)
(67, 65, 25, True)
(67, 65, 34, True)
(67, 65, 36, True)
(67, 65, 38, True)
(67, 65, 48, True)
(67, 65, 55, True)
(67, 65, 61, True)
(67, 65, 63, True)
(71, 41, 31, True)
(71, 69, 2, True)
(71, 69, 3, True)
(71, 69, 4, True)
(71, 69, 5, True)
(71, 69, 7, True)
(71, 69, 9, True)
(71, 69, 11, True)
(71, 69, 17, True)
(71, 69, 19, True)
(71, 69, 26, True)
(71, 69, 28, True)
(71, 69, 31, True)
(71, 69, 37, True)
(71, 69, 39, True)
(71, 69, 44, True)
(71, 69, 49, True)
(71, 69, 59, True)
(79, 25, 9, True)
(79, 25, 63, True)
(79, 25, 66, True)
(79, 77, 3, True)
(79, 77, 9, True)
(79, 77, 10, True)
(79, 77, 12, True)
(79, 77, 17, True)
(79, 77, 19, True)
(79, 77, 20, True)
(79, 77, 21, True)
(79, 77, 22, True)
(79, 77, 24, True)
(79, 77, 37, True)
(79, 77, 39, True)
(79, 77, 41, True)
(79, 77, 43, True)
(79, 77, 45, True)
(79, 77, 50, True)
(79, 77, 51, True)
(79, 77, 63, True)
(79, 77, 66, True)
(83, 81, 2, True)
(83, 81, 8, True)
(83, 81, 10, True)
(83, 81, 11, True)
(83, 81, 22, True)
```

```
(83, 81, 24, True)
(83, 81, 26, True)
(83, 81, 27, True)
(83, 81, 28, True)
(83, 81, 29, True)
(83, 81, 30, True)
(83, 81, 32, True)
(83, 81, 37, True)
(83, 81, 39, True)
(83, 81, 50, True)
(83, 81, 60, True)
(83, 81, 62, True)
(83, 81, 64, True)
(83, 81, 69, True)
(83, 81, 76, True)
```

Se puede verificar que en el output anterior salen todas las involuciones de $P(x)$ para $q = 4k + 3$

In [ ]:

# Binomios de Involucion en F_p con dmc(m,q-1)=2

June 8, 2018

## 1 Lillian González Albino

### 1.1 Binomios de involución con $dmc(m, q-1) = 2$

En el paper del Dr. Wan Daqing, se encontró que los binomios de involución pueden tener $gcd(m, q-1) = 1$ o $gcd(m, q-1) = 2$. A continuación se encuentra el código utilizado para crear conjeturas sobre los binomios de involución con $dmc(m, q-1) = 2$. Es importante notar que las permutaciones con $dmc(m, q-1) = 2$, según el teorema del Dr. Wan, son solo con $q = 4k + 3$.

Funciones para construir permutaciones con $dmc(m, q-1) = 2$

```
In [2]: #input: q primo
        #output: lista de enteros
        #recibe un primo q y devuelve una lista de todas las m
        #que sean relativamente primas a q-1

        def findMs(q):
            listOfMs = []
            for m in range(q):
                if(gcd(m,q-1)==2):
                    listOfMs.append(m)
            return listOfMs

        #input: int
        #output: list of ints
        #Coge un primo p y te devuelve una lista de los quadratic
        #non residues mod p
        def quadratic_nonresidues(p):
            NQR = set(range(p)) - set(quadratic_residues(p))
            return list(NQR)

        #input: q primo
        #output: lista de enteros
        #recibe un primo q y devuelve una lista de todas las a que
        #satisfacen que a^2-1 es un residuo cuadratico mod q

        def findAs(q):
            listOfAs =[]
            NQR = quadratic_nonresidues(q)
            for a in range(q):
                if((a^2-1)%q in NQR):
                    if(a != 0 and (a^2-1)%q != 0):
                        listOfAs.append(a)
            return listOfAs
```

```
#input: primo q, int a, int m
#output: bool
#recibe un primo q, una a y una m y verifica si el polinomio
#con las dadas variables es de permutacion

def checkifPP(q,a,m):
    A = range(q)
    B = []
    for x in A:
        P = x^m * (x^((q-1)/2) + a)
        B.append(P%q)
    if(set(A) == set(B)):
        return True
    else:
        return False

#input: primo q, lista de enteros lA, lista de enteros lM
#output: void
#recibe un primo q y una lista de as y ms y verifica si todas
#las combinaciones de as y ms (bajo mod q) son polinomios de
#permutacion. Despliega las combinaciones (q,m,a) que no sean
#de permutacion

def checkPP(q):
    lA = findAs(q)
    lM = findMs(q)
    for a in lA:
        for m in lM:
            if(checkifPP(q,a,m)==False):
                print(q,a,m)

#input: int, int
#output: void
#recibe un primo frm y verifica si los proximos n primos son PP
def checkAllPP(frm, n):
    P = Primes()
    p = frm -1
    for i in range(n):
        p = P.next(p)
        if(findPform(p)==3):
            checkPP(p)
```

Función para encontrar la forma de $q$, ($q = 4k + 1$ o $q = 4k + 3$)

In [3]:
```
#input: p primo
#output: 1,3
#coge un primo p y devuelve 1 si p=4k+1 y, 3 si p=4k+3
def findPform(p):
    pForm = 0
    if(((p-1) % 4) == 0):
        pForm = 1
    if(((p-3) % 4) == 0):
        pForm = 3
    return pForm
```

Ya verificamos si el binomio era de permutación en $\mathbb{F}_q$ ahora vamos a verificar las involuciones

In [4]:
```
#input: p primo, int m, int a
#output: bool
#recibe un p primo, int m, int a, y verifica si el binomio
#con las dadas variables es de involucion
#add verificar puntos fijos > 0

def checkifInv(p,m,a):
    h = (p-1)/2
    d = 0
    for x in range(1,p+1):
        Px = ( x^m * (x^h + a) )%p
        PPx = ( Px^m * (Px^h + a) )%p
        if(Px == x):
            d += 1
        if(PPx == 0):
            PPx = p
        if(PPx != x):
            return False
    if(d > 0):
        return True
    else:
        return False

#input: p primo
#output: lista (int, int, int)
#recibe un primo p y calcula todas las involuciones de esa p
#y devuelve una lista con elementos tuplas (p,m,a) que hacen
#el binomio una involucion

def findAllInv(p):
    lM = findMs(p)
    lA = findAs(p)
    lInv = []
    for m in lM:
        for a in lA:
            if(checkifInv(p,m,a)):
                lInv.append((p,m,a))
    return lInv

#input: int frm, int n
#output: void
#verifica todas las involuciones desde el proximo primo despues de
#frm y los proximos n primos despues de from y despliega las
#combiaciones (p,m,a) de involuciones.

def findInvolution(frm, n):
    P = Primes()
    p = frm -1
    for i in range(n):
        p = P.next(p)
        if(findPform(p)==3):
            for elem in findAllInv(p):
```

```
                print(elem)
```

Función para verificar proposiciones para n primos

```
In [5]: #input: int frm, int n
        #output: void
        def checkProps(func, frm, n):
            P = Primes()
            p = frm -1
            for i in range(n):
                p = P.next(p)
                if(findPform(p)==3):
                    func(p)
```

Verificar conjetura 1: Sea $dmc(m, q-1) = 2$. Si $\eta(a^2-1) = -1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{\frac{q-1}{2}} = 1$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [6]: #input: p primo
        #output: void
        # verifica la conjetura: gcd(m,p-1)==1 y a^2-1 r.c. y
        #m^2 congr 1 (mod) (p-1)/2 y (a+1)^((p-1)/2) % p == 1  => involucion
        def prop1(p):
            lA = findAs(p)
            for m in range(p):
                if(gcd(m, p-1)==2): #gcd 2
                    halfp = (p-1)/2
                    if(m^2 % halfp == 1): #m^2 = 1
                        for a in lA:
                            plusa = a+1
                            if(plusa^halfp % p == 1): #a+1 QR
                                print(p,m,a,checkifInv(p,m,a)) #check if inv
```

La proposición 1 nos devuelve todas las involuciones, pero incluso devuelve tuplas de (p,m,a) que no generan involuciones.

Verificar conjetura 2: Sea $dmc(m, q-1) = 2$. Si $\eta(a^2-1) = -1$ y $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$ y $(a+1)^{\frac{q-1}{2}} = 1$ y $(a+1)^{m+1} = 1$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [7]: #input: p primo
        #output: void
        # verifica la conjetura: gcd(m,p-1)==1 y a^2-1 r.c. y
        #m^2 congr 1 (mod) (p-1)/2 y (a+1)^((p-1)/2) % p == 1  => involucion
        def prop2(p):
            lA = findAs(p)
            for m in range(p):
                if(gcd(m, p-1)==2): #gcd 2
                    halfp = (p-1)/2
                    if(m^2 % halfp == 1): #m^2 = 1
                        for a in lA:
                            plusa = a+1
                            if(plusa^halfp % p == 1): #a+1 QR
                                expo = m+1
                                if(plusa^expo % p == 1): #a+1^m+1
                                    print(p,m,a,checkifInv(p,m,a)) #check if inv
```

La proposición 2 nos devuelve todas las involuciones, pero incluso devuelve tuplas de (p,m,a) que no generan involuciones.

Verificar conjetura 3: Sea $dmc(m, q-1) = 2$. Si $\eta(a^2-1) = -1$, $m^2 \equiv 1 \ (mod \ \frac{q-1}{2})$, $(a+1)^{\frac{q-1}{2}} = 1$, $(a+1)^{m+1} = 1$ y $(a-1)^{m+1} = -1$, entonces P(x) es involución en $\mathbb{F}_q$

Todo reducido mod $q$

```
In [8]: #input: p primo
        #output: void
        # verifica la conjetura 3
        def prop3(p):
            lA = findAs(p)
            for m in range(p):
                if(gcd(m, p-1)==2): #gcd 2
                    halfp = (p-1)/2
                    if(m^2 % halfp == 1): #m^2 = 1
                        for a in lA:
                            plusa = a+1
                            if(plusa^halfp % p == 1): #a+1 QR
                                expo = m+1
                                if(plusa^expo % p == 1): #a+1^m+1
                                    minusa = a-1
                                    if(minusa^expo % p == p-1): #a-1^m+1
                                        print(p,m,a,checkifInv(p,m,a)) #check if inv
```

Con la conjetura 3 tenemos todas las involuciones con gcd 2

```
In [9]: #restringe output a solo las tuplas que cumplen con las condiciones de la prop.3
        checkProps(prop3, 3, 15)
```

```
(11, 4, 3, True)
(11, 4, 8, True)
(19, 8, 3, True)
(19, 8, 4, True)
(19, 8, 15, True)
(19, 8, 16, True)
(23, 10, 8, True)
(23, 10, 11, True)
(23, 10, 12, True)
(23, 10, 15, True)
(31, 14, 4, True)
(31, 14, 7, True)
(31, 14, 13, True)
(31, 14, 18, True)
(31, 14, 24, True)
(31, 14, 27, True)
(43, 20, 3, True)
(43, 20, 8, True)
(43, 20, 9, True)
(43, 20, 13, True)
(43, 20, 20, True)
(43, 20, 23, True)
(43, 20, 30, True)
(43, 20, 34, True)
(43, 20, 35, True)
(43, 20, 40, True)
```

```
(43, 34, 3, True)
(43, 34, 40, True)
(47, 22, 6, True)
(47, 22, 11, True)
(47, 22, 16, True)
(47, 22, 20, True)
(47, 22, 23, True)
(47, 22, 24, True)
(47, 22, 27, True)
(47, 22, 31, True)
(47, 22, 36, True)
(47, 22, 41, True)
```

In [10]:
```
#genera todas las involuciones con dmc(m,q-1)=2
findInvolution(3, 15)
```

```
(11, 4, 3)
(11, 4, 8)
(19, 8, 3)
(19, 8, 4)
(19, 8, 15)
(19, 8, 16)
(23, 10, 8)
(23, 10, 11)
(23, 10, 12)
(23, 10, 15)
(31, 14, 4)
(31, 14, 7)
(31, 14, 13)
(31, 14, 18)
(31, 14, 24)
(31, 14, 27)
(43, 20, 3)
(43, 20, 8)
(43, 20, 9)
(43, 20, 13)
(43, 20, 20)
(43, 20, 23)
(43, 20, 30)
(43, 20, 34)
(43, 20, 35)
(43, 20, 40)
(43, 34, 3)
(43, 34, 40)
(47, 22, 6)
(47, 22, 11)
(47, 22, 16)
(47, 22, 20)
(47, 22, 23)
(47, 22, 24)
(47, 22, 27)
(47, 22, 31)
(47, 22, 36)
(47, 22, 41)
```

In [ ]: