TRABAJO FINAL
MAESTRÍA EN MATEMÁTICAS

POLINOMIOS PERFECTOS SOBRE F_2

Por:

VALERIA CELY ROJAS

Código: 830204

Director:

VÍCTOR SAMUEL ALBIS GONZÁLEZ.

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÀTICAS
BOGOTÁ 2010

Valeria Cely Rojas

Víctor Samuel Albis

TABLA DE CONTENIDO

1. INTRODUCCIÓN

1. Sobre los números enteros perfectos. En la proposición 36 del libro IX de los *Elementos* de **Euclides** [7] se lee:

"Si varios números, empezando por la unidad, están en proporción duplicada y el conjunto de todos es un número primo, el producto de este conjunto por el último es un número perfecto".

En la notación de la época, **Euclides** se está refiriendo al fascinante tema de los números perfectos, en particular, la proposición 1, *infra,* contiene en lenguaje moderno la proposición de Euclides. Pero, ¿qué es un número perfecto? Es aquel que es igual a la suma de sus divisores propios. Con otras palabras, el número *n* es perfecto si $\sum_{\substack{d|n \\ d\neq n}} d = n$. O equivalentemente $\sigma(n) = \sum_{d|n} d = 2n$.

El siguiente lema contiene una propiedad trivial de los números enteros perfectos

Lema 1. *Si n es perfecto entonces* $n|\sigma(n)$.

Demostración. Si *n* es perfecto entonces $2n = \sigma(n)$ implica que $n|\sigma(n)$. □

Los divisores propios de 6 son 1, 2 y 3 y se tiene que 1 + 2 + 3 = 6, es decir, 6 es un número perfecto. La proposición de Euclides contiene una fórmula que genera números perfectos pares y que, en notación moderna, afirma que el número

$$2^{k-1}(2^k - 1)$$

es perfecto siempre que $2^k - 1$ sea primo. En el siglo XVIII **Euler** demostró el recíproco de la proposición. Esto es, que todo número perfecto par satisface la fórmula enunciada por Euclides. Más precisamente, tenemos el siguiente resultado:

Proposición 1. Un número par *n* es perfecto cuando, y sólo cuando,

$$n = 2^{q-1}(2^q - 1),$$

donde *q* y $2^q - 1$ son números primos.

Demostración. Observemos en primer lugar que si $2^n - 1$ es primo, entonces *n* es primo. En efecto, si *n = ab*, con *a, b* > 1, vemos que $(2^a - 1)|(2^a)^b - 1 = 2^n - 1$, lo cual no es posible porque, por hipótesis, $2^n - 1$ es primo. Pasemos, ahora sí, a la demostración de la proposición: podemos escribir $n = 2^r m$, con *m* impar y *r > 0*. Luego,

$$2^{r+1}m = 2n = \sum_{d|n} d = \sigma(n) = \sigma(2^r)\sigma(m) = (2^{r+1} - 1)\sigma(m),$$

puesto que σ es multiplicativa (véase [17]). Como $(2^{r+1}-1, 2^{r+1}) = 1$, tenemos $2^{r+1}-1|m$, de modo que $m = s(2^{r+1}-1)$, para algún entero *s*. Entonces

$$\sigma(m) \geq s(2^{r+1}-1) + s = s2^{r+1};$$

por otra parte,

$$s(2^{r+1}-1)2^{r+1} = 2^{r+1}-1\ \sigma(m) \text{ implica que } \sigma(m) = s2^{r+1}.$$

En consecuencia, *s* y $s(2^{r+1}-1)$ y son los únicos divisores de *m*, lo cual fuerza a que *s* = 1 y *m* = $2^{r+1}-1$ sea primo. Por lo tanto,

$$n = 2^r(2^{r+1}-1) = 2^{q-1}(2^q-1),$$

si hacemos $q = r + 1$. Pero ya hemos visto que en este caso, q es primo. Recíprocamente, si $n = 2^{q-1}(2^q-1)$, con q y 2^q-1 1 primos, es claro que

$$\sigma(n) = \sigma(2^{q-1})\sigma(2^q-1) = [(2^q-1)+1](2^q-1) =$$

$$2^q(2^q-1) = 2[2^{q-1}(2^q-1)] = 2n. \square$$

En su *Isagoge o Introducción a la aritmética,* **Nicómaco de Gerasa** (siglo II de J. C.), sin prueba alguna dice, que los siguientes hechos, expresados en la terminología moderna, son verdaderos:

a. El *n* –ésimo número perfecto tiene *n* dígitos.
b. Todos los números perfectos son pares.
c. Todos los números perfectos terminan alternadamente en 6 y en 8.
d. Todo número perfecto es de la forma $2^{q-1}(2^q-1)$, para algún *q,* si 2^q-1 es primo.
e. Existe una cantidad infinita de números perfectos.

Ahora bien, para la época de **Nicómaco** los únicos números perfectos conocidos eran: 6, 28, 496, 8.128, de modo que sus aseveraciones, al parecer, son el fruto de una ingenua *inducción baconiana.* Así, el quinto número perfecto (calculado por **Jámblico** y descubierto, por **Curtze** en un manuscrito latino) es:

$$2^{12}(2^{13}-1) = 33.550.336,$$

el cual tiene 8 dígitos. Esto invalida a. Por otra parte. **Pietro Antonio Cataldi** (1548-1626), en 1603, encontró el sexto número perfecto:

$$2^{16}(2^{17}-1) = 8.589.869.056,$$

con lo cual invalidó la alternancia del 6 y del 8 como dígitos finales de los números perfectos expresados en c. Sin embargo, más adelante (proposición 2), mostraremos que el último dígito de un número perfecto par necesariamente es 6 u 8. En cuanto a d., ya observamos, en la demostración de la proposición 1, que si $2^q - 1$ es primo entonces q es primo y que, en tal caso, $2^{q-1}(2^q - 1)$, es un número perfecto par. Luego d. no puede aplicarse como criterio para determinar si existen o no números perfectos impares. El que hasta hoy no se haya encontrado un número perfecto impar ha conducido a la siguiente conjetura:

No existen números perfectos impares.

Sin embargo, se han encontrado varias condiciones que deberían cumplir los números perfectos impares. Por ejemplo, **Muskat** [16] ha mostrado lo siguiente: *Si n es un número perfecto impar, entonces n tiene un divisor de la forma* $p^m > 10^{12}$*, donde p es un número primo.* De manera que si *n* es perfecto e impar, *n* debe ser bastante grande. Por otra parte, **Hagis** [11] (1980) demostró que un número perfecto impar debe tener al menos 8 factores primos diferentes.

En la misma dirección, es decir, en la búsqueda de un eventual número perfecto impar o de sus factores primos, están los siguientes trabajos: [2], [3], [12] y [14].

El resultado que demostramos en seguida resulta de ayuda cuando queremos verificar si un número par es o no perfecto.

Proposición 2*. Si n es un número perfecto par, entonces su último dígito es o bien 6 o bien 8*.

Demostración. Sabemos que $n = 2^{q-1}(2^q - 1)$, donde q es un primo. Si *q=2,* entonces *n=6*. Supongamos, pues, que *q* es impar. Por el teorema de Fermat tenemos $2^4 \equiv 1(mód\ 5)$. Como *q-1* es par, entonces *q-1= 4m* o *q-1=4m+2,* para algún $m \in \mathbb{Z}$. Consideremos la primera posibilidad. En este caso:

$$2^{q-1} = (2^4)^m \equiv 1\ (mód\ 5)$$

$$2^q - 1 = \ 2^{q-1} \cdot 2 - 1 \equiv 2 - 1 \equiv (mód\ 5)$$

es decir,

$$n \equiv 1(mód\ 5)$$

$$n \equiv 1 \text{ ó } 6(mód\ 10).$$

Como *n* es par, por fuerza $n \equiv 6(mód\ 10)$. Si *q-1 = 4m+2,* tenemos

$$2^{q-1} = (2^4)^m 2^2 \equiv 4\ (mód\ 5)$$

$$2^q - 1 = \ 2^{q-1} \cdot 2 - 1 \equiv 7(mód\ 5),$$

es decir,

$$n \equiv 4 \cdot 7 \equiv 3(mód\ 5)$$

$$n \equiv 3 \text{ ó } 8(mód\ 10).$$

Como *n* es par, forzosamente $n \equiv 8(mód\ 10)$. □

2. El análogo de los números perfectos en los anillos de polinomios. Uno de los campos de la matemática que ha llamado la atención desde mediados del siglo pasado es la teoría aritmética de los polinomios. Esta teoría traslada cuestiones de la teoría de números en el anillo Z de los números enteros a sus análogas en el anillo $F_q[x]$ de los polinomios en la indeterminada *x* y coeficientes en un cuerpo finito F_q de *q* elementos. (Véase [1])

Quien primero introdujo y estudió en este contexto el concepto de polinomios perfectos fue **E. F. Canaday** en su tesis doctoral, bajo la supervisión de **Leonard Carlitz** (de hecho **Canaday** fue su primer estudiante doctoral de un total de 45).

Canaday en su artículo "The sum of divisors of a polynomial" (1941) (resultante de su tesis) desarrolló ideas originales sobre el tema, restringiéndolo a los polinomios unitarios en $F_2[x]$. Si $(A, x + x^2) = 1$ dice que *A* es impar y par en caso contrario.

En los últimos años, **Luis H. Gallardo** y **Olivier Rahavandrainy** han abanderado el estudio de los polinomios perfectos en $F_q[x]$ con *q* en {2, 3, 4}, mostrando un interesante desarrollo de las ideas introducidas originalmente por **Canaday.**

Entre sus resultados se destacan los siguientes:

- La caracterización de los polinomios perfectos $A \in F_4[x]$ con cuatro divisores primos, donde uno de ellos tiene grado 1, como se muestra en el artículo: "Perfect polynomials over F_4 with less than five prime factors" (2007).

- Por otra parte, en el artículo “Perfect polynomials over F_3” (2008) exponen la no existencia de polinomios perfectos impares con tres divisores primos, es decir de la forma $A = P^h Q^k R^l$ donde P, Q y R son polinomios unitarios irreducibles diferentes sobre F_3, usando que A es un polinomio perfecto impar (*vide infra*) sobre F_3 si $(A, x^3 - x) = 1$.
- En “Odd perfect polynomials over F_2” (2007) encuentran resultados para una clase especial de polinomios perfectos impares.

El propósito de nuestro trabajo es estudiar los resultados de este último artículo.

2. PRELIMINARES

1. El anillo de los polinomios en una indeterminada con coeficientes en un campo.

En esta sección recordaremos algunos resultados sobre los anillos de polinomios en una indeterminada con coeficientes en un campo, que en general suponemos finito.

El siguiente teorema lo usaremos con alguna frecuencia, sobre todo en el caso de característica 2:

Teorema 1. Sea K un cuerpo de característica $p > 0$ entonces se cumple la identidad

$$(x + y)^p = x^p + y^p \ .$$

Demostración. Tenemos, usando el binomio de Newton, que:

$$(x + y)^p = x^p + px^{p-1}y + \frac{p(p-1)}{2!}x^{p-2}y^2 + \frac{p(p-1)(p-2)}{3!}x^{p-3}y^3 + \cdots + pxy^{p-1} + y^p.$$

Como p es la característica de K y como $p|\binom{p}{k}, k = 1,\cdots, p-1$, por lo tanto

$$(x + y)^p = x^p + y^p. \square$$

Aplicando inducción sobre n se tiene:

$$(x_1 + \cdots + x_n)^p = x_1^p + \cdots + x_n^p$$

Sabemos que si F es un campo, el anillo $F[x]$ de los polinomios de coeficientes en F en la indeterminada x es un anillo de factorización única, cuyas unidades son los polinomios constantes distintos de cero. Para $A(x), B(x) \in F[x], A(x) \sim B(x)$ significa que existe una unidad u del anillo $F[x]$ tal que $A(x) = uB(x)$; esta relación $\sim$ es claramente una relación de equivalencia. Es fácil verificar que en cada clase de equivalencia según esta relación existe un único polinomio de coeficiente director 1, o como también se dice un polinomio unitario, que la representa. Por esta razón solo consideraremos polinomios unitarios, que son los análogos correctos en $F[x]$ de los números enteros positivos. El conjunto de los polinomios unitarios de $F[x]$ lo designamos con $M(F, x)$. Es claro que $F_2[x] = M(F_2, x)$.

Con estas convenciones **el** máximo común divisor de dos polinomios unitarios P y Q siempre existe y es entonces un polinomio unitario, el cual denotamos con $(P, Q) = 1$. En efecto, si $P = P_i^{\alpha_1} \ldots P_s^{\alpha_s}, Q = P_i^{\beta_1} \ldots P_s^{\beta_s}, 0 \leq \alpha_{i,} \beta_i$ y los P_i son primos; entonces $(Q, P) = P_i^{\delta_1} \ldots P_s^{\delta_s}$ donde $\delta_i = mín\{\alpha_i, \beta_i\}$ (véase [1]).

Definición 1. Dos polinomios $P, Q \in M(F, x)$ se dicen primos relativos o primos entre sí, sí su máximo común divisor es 1.

La demostración del siguiente teorema aparece en [13].

Teorema 2. Dos polinomios $R(x), S(x) \in M(F, x)$ son relativamente primos, si y sólo si se tiene $T(x)R(x) + U(x)S(x) = 1$ para ciertos $T(x), U(x) \in M(F, x)$.

El siguiente teorema es muy conocido y su demostración se puede encontrar en [13]

Teorema 3. (*Teorema del factor****)*** Un polinomio $f(x) \in F[x]$ admite como factor a $(x - k)$ si, y sólo si, *k* es una raíz de $f(x)$, es decir que $f(k) = 0$.

Análogamente al caso de los enteros decimos que una función *f:* $M(F, x) \to \mathbb{C}$ es una *función aritmética.*

Definición 2. Una función aritmética f se dice **multiplicativa** si no es idénticamente nula y si $f(PQ) = f(P)f(Q)$ cuando $(P, Q) = 1$.

Un ejemplo de una función aritmética multiplicativa es

$$\sigma(A) = \sum_{D|A} D,$$

donde *D* recorre los divisores unitarios del polinomio *A* en $M(F, x)$. Una demostración de este hecho se encuentra [1].

La función aritmética $w(A) = \sum_{\substack{P|A \\ P\ irreducible}} 1$, indica el número de polinomios irreducibles que dividen a A. También es multiplicativa. [1]

De acuerdo con el *lema 1,* del capítulo 1, la siguiente parece ser una buena generalización de la noción de polinomios perfectos en $F_2[x]$

Definición 3. Un ***polinomio unitario*** *A* sobre F_2 se dice ***perfecto*** si $A|\sigma(A)$.

Esto es equivalente a que $\sigma(A) = A$. En efecto; si $A|\sigma(A)$ entonces $\sigma(A) = 1 + \cdots + A = AQ$, como $gr(A) = gr(A) + gr(Q)$ resulta que $gr(Q) = 0$; es decir, Q es una constante diferente de cero y el único polinomio constante en F_2 distinto de cero es 1.

Observemos que esta definición difiere de la usada en el caso de los enteros. La razón de esto estriba en que 2 = 0 en los campos de característica 2.

Definición 4. Sea F un campo y $A \in M(F,x)$**.** Dada la descomposición de A en polinomios primos unitarios, los polinomios de menor grado que aparecen en ella, se llaman ***polinomios primos minimales***. Los ***polinomios primos maximales*** se definen de manera análoga. Cuando el divisor primo de A no es ni minimal ni maximal se dice un ***primo medial*** de A.

Definición 5. Un polinomio $A \in F_2[x]$ se dice impar si $(A, x+x^2) = 1$ y par si $(A, x+x^2) \neq 1$. O lo que es equivalente a es impar si $(A, x+1) = 1$ y $(A, x) = 1$.

Definición 6. Un polinomio perfecto impar $A \in F_2[x]$se dice "***perfecto especial***" si es un producto de $m = w(A)$ primos $P_i \in F_2[x]$ de grado d_i con exponentes todos iguales a 2. Es decir,

$$A = P_1^2 \dots P_m^2 \text{ donde } 2 \leq d_1 \leq \cdots \leq d_m .$$

Además como $A = \sigma(A)$ se tiene la identidad

$$\sigma(P_1^2) \cdots \sigma(P_m^2) = P_1^2 \dots P_m^2.$$

Lema 1*:* Sea $P \in F_2[x]$ y α raíz de P, entonces α^2 también es raíz de P.

Demostración: Sea $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F_2[x]$ y α raíz de P; entonces

$$P(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

Por otra parte, y dado que, por el pequeño teorema de Fermat, $a = a^2$, podemos escribir ahora

$$P(\alpha^2) = \alpha^{2n} + a_{n-1}^2 \dots + a_0{}^2;$$

y como consecuencia del teorema 1 tenemos que:

$$P(\alpha^2) = (\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0)^2 = 0. \square$$

3. ESTUDIO DE LOS POLINOMIOS PERFECTOS IMPARES SOBRE F_2.

1. Algunos lemas preliminares

Los siguientes lemas generalizan los lemas 5 y 6 en [2], respectivamente, enunciados para $F_{2,}$ al demostrarlos para todo campo de característica 2.

Lema 1. *Sea F un campo de característica 2. Sean* $P, Q \in M(F, x), P$ *irreducible y* $n, m \in \mathbb{N}$ *tales que*

$$1 + P + \cdots P^{2n-1} + P^{2n} = Q^m \tag{1}$$

entonces $m \in \{0,1\}$.

Demostración. Veamos que m no puede ser par, ya que si lo fuera se tendría *m = 2k,* de modo que

$$Q^m = Q^{2k} = (Q^k)^2 = (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)^2;$$

ahora, utilizando el teorema 1 del capítulo 2, se obtiene:

$$Q^m = a_0^2 + a_1^2x^2 + a_2^2x^4 + \cdots + a_n^2x^{2n},$$

donde todas las potencias de *x* son pares. Por otra parte, en (1) el lado izquierdo contiene necesariamente potencias impares de *x* pues al ser *P* irreducible no puede contener exclusivamente potencias pares ya que como consecuencia del mencionado teorema, *P* sería factorizable. Luego, es imposible que *m* sea par.

Por otra parte, de (1) resulta

$$P^{n+1}(P^{n-1} + P^{n-2} + \cdots + 1) + P\,(P^{n-1} + P^{n-2} + \ \ldots + 1) + 1 = Q^m,$$

es decir,

$$(P^{n-1} + P^{n-2} + \cdots + 1)(\,P^{n+1} + P) + 1 = \ Q^m;$$

entonces

$$(P^{n-1} + P^{n-2} + \cdots + 1)(\,P^{n+1} + P) + Q^m = \ 1 \tag{2}$$

Luego, en virtud del teorema 2, del capítulo 2, se tiene

$$(Q, (P^{n-1} + P^{n-2} + \cdots + 1)) = 1. \qquad (3)$$

Derivando (1) , se obtiene:

$$P'(2n\,P^{2n-1} + (2n-1)P^{2n-2} + (2n-2)P^{2n-3} + \cdots + 1) = Q'mQ^{m-1}$$

Es claro que el término del lado derecho es igual a $Q'Q^{m-1}$, ya que m es impar. Como se está sobre un campo de característica 2 entonces:

$$P'(\,P^{2(n-1)} + P^{2(n-2)} + \cdots + 1) = Q'Q^{m-1};$$

aplicando el teorema 1del capítulo 2, se tiene:

$$P'(\,P^{n-1} + P^{n-2} + \cdots + 1)^2 = Q'Q^{m-1}.$$

Como consecuencia de (3) se concluye que:

$$Q^{m-1} \nmid (P^{n-1} + P^{n-2} + \cdots + 1)^2$$

y, por lo tanto, $Q^{m-1} \mid P'$. Luego, $gr(P') \geq gr(Q^{m-1})$, o sea:

$$gr(P) > gr(P') \geq (m-1)gr(Q);$$

multiplicando a ambos lados por 2n, vemos que

$$2ngr(P) > 2n(m-1)gr(Q). \qquad (4)$$

De (1) se tiene:

$$mgr(Q) = 2ngr(P);$$

reemplazando en (4), obtenemos:

$$mgr(Q) > 2n(m-1)gr(Q)$$

y

$$m > 2n(m-1)\,. \qquad (5)$$

Como $n \geq 1$, entonces 2n (m - 1) ≥ 2(m - 1) y por (5) se tiene:

$$m > 2(m-1)\,,$$

$$m > 2m-2\,,$$

$$2 > m;$$

en conclusión: $m \in \{0,1\}$. □

Lema 2. *Sea F un campo de característica 2. Sean $P, Q \in F[x], P$ irreducible y $n, m \in \mathbb{N}$ tales que $m > 1$ y $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m A$ para algún $A \in F[x]$. Entonces $gr(P) > 2gr(Q)$.*

Demostración. Derivando $1 + \cdots + P^{2n} = Q^m A$, como se realizó en la prueba del lema anterior, se tiene:

$$P'(P^{n-1} + P^{n-2} + \cdots + 1)^2 = mQ'Q^{m-1}A + Q^m A'. \qquad (6)$$

Si $m = 2$ se obtiene de (6) que:

$$P'(P^{n-1} + P^{n-2} + \cdots + 1)^2 = Q^2 A';$$

luego,

$$Q^2 \mid P',$$

y, por consiguiente,

$$2gr(Q) \leq gr(P') < gr(P).$$

En conclusión:

$$2gr(Q) < gr(P). \square$$

***Lema* 3.** *Sea $A \in F_2[x]$ un polinomio perfecto. Entonces el número de primos minimales unitarios de A es par.*

Demostración. Sea $P_1, \ldots, P_r$ la lista de todos los primos minimales unitarios de A. Como A es un polinomio perfecto entonces: $\sigma(A) = A$, es decir,

$$\sum_{d|A} d = A.$$

Por consiguiente,

$$\sum_{\substack{d|A \\ d \neq A}} d + (A - A) = 0,$$

o sea,

$$0 = \sum_{\substack{d|A \\ d \neq A}} d = \sum_{i=1}^{r} \frac{A}{P_i} + \cdots .$$

Tomando los primeros términos del lado derecho de esta igualdad se tiene:

$$\frac{A}{P_1} + \cdots + \frac{A}{P_r} = rx^{gr(A)-gr(P_i)} + \cdots = 0$$

En consecuencia *r* es par. □

2. Polinomios perfectos en $F_2[x]$ de la forma $A = P^h Q^k R^l$ donde P, Q y R son primos.

Podemos suponer que P y Q son primos minimales unitarios ya que, por el anterior lema 3, la cantidad de primos minimales unitarios de A es un número par; por lo tanto,

$$gr(P) = gr(Q) < gr(R).$$

Como P y Q, h y k juegan papeles análogos, si $gr(P) = gr(Q) = 1$ y como P y Q son irreducibles uno de ellos es x y el otro es x+1. Por lo tanto, A es par.

Si fuese $gr(P) = gr(Q) \geq 2$, entonces A sería impar, pues en caso contrario A tendría un factor igual a x o igual a $x + 1$, lo cual implicaría que alguno de los P, Q o R sería factorizable. Teniendo en cuenta lo anterior podemos demostrar el siguiente:

Teorema 4. *Si $A = P^h Q^k R^l$ es un polinomio perfecto en $F_2[x]$ con tres factores irreducibles P, Q, R entonces al menos alguno de ellos es de grado 1.*

Demostración. Supongamos que P, Q y R son todos de grado mayor o igual que 2. Si A es un polinomio perfecto entonces, utilizando la multiplicidad de σ se tiene:

$$\sigma(A) = \sigma(P^h Q^k R^l) = \sigma(P^h)\sigma(Q^k)\sigma(R^l) = A,$$

o sea:

$$(1 + \cdots + P^h)(1 + \cdots + Q^k)(1 + \cdots + R^l) = P^h Q^k R^l,$$

donde:

$$1 + \cdots + P^h = \frac{P^h Q^k R^l}{(1+\cdots+Q^k)(1+\cdots+R^l)} = P^c Q^a R^b; \qquad (7)$$

tomando el lado izquierdo de (7) se tiene:

$$1 + P + P^2 + \cdots + P^h = 1 + P(1 + P + \cdots + P^{h-1})$$

de lo cual concluimos que $1 + P + P^2 + \cdots + P^h$ no es divisible por P; por lo tanto, P no es factor de (7). Es decir,

$$1 + \cdots + P^h = Q^a R^b \quad . \tag{8}$$

De manera análoga se obtienen las relaciones:

$$1 + \cdots + Q^k = P^c R^d \quad , \tag{9}$$

$$1 + \cdots + R^l = P^e Q^f \quad , \tag{10}$$

de donde $Q^a R^b P^c R^d P^e Q^f = P^{c+e} Q^{f+a} R^{b+d} = P^h Q^k R^l$ y, por lo tanto,

$$\left.\begin{array}{l} c + e = h, \\ a + f = k, \\ b + d = l. \end{array}\right\} \tag{11}$$

Caso en que alguno $h, k, ó, l$ sea impar:

Supongamos que h sea impar. Necesariamente $P(0) = 1$, ya que en caso contrario, por el teorema del factor, x sería factor de P. Entonces se tiene $1 + P(0) + \cdots + P(0)^h = h + 1 = 0$ pues $h + 1$ es par y estamos en característica 2. Entonces, x divide a $1 + \cdots + P^h$. Esto implica, según (8), que x divide a $Q^a R^b$; entonces $x \mid Q$ o $x \mid R$, y como Q y R son irreducibles tendríamos $Q = x$, o, $R = x$; como $gr(Q) < gr(R)$, necesariamente $Q = x$, y, por lo tanto, hay al menos un factor de grado 1. De manera análoga se tiene esto si k *ó* l son impares.

Veamos ahora que el caso anterior es el único posible.

Caso en el cual $h, k,$ y l son todos pares:

Supongamos que $a > 1$. Entonces si aplicamos el lema 2 a (8) tomando a R^b como A obtenemos $gr(P) > 2gr(Q)$ lo cual constituye una contradicción ya que $gr(P) = gr(Q)$. Por consiguiente, $0 \leq a \leq 1$. De forma análoga se tiene que $0 \leq b, c, d \leq 1$. Si $b = 0$, aplicando el lema 1 a (8) se tendría $a = 1$ y así $h = 1$ ya que $gr(P) = gr(Q)$, lo cual es imposible porque estamos en el caso en que h es par; en conclusión, $b = 1$.

De forma análoga se tiene que $d = 1$, de modo que $l = b + d = 2$.

Si $a = c = 1$, entonces $h = k, e = h - 1 = k - 1 = f$. Por consiguiente, $1 + R + R^2 = (PQ)^e$. Así, por el lema 2, $e = 1$ y $h = 2$. Entonces se tiene:

$$1 + P + P^2 = QR,$$

donde $2gr(P) = gr(Q) + gr(R)$ y teniendo en cuenta que $gr(Q) = gr(P)$, entonces $gr(P) = gr(R)$ y, así, P, Q y R tienen el mismo grado, lo cual es una contradicción. Si $a = 0, c = 1$, entonces

$$1 + \cdots + P^h = R,$$

$$1 + \cdots + Q^k = PR.$$

Luego,

$$hgr(P) = gr(R),$$

$$kgr(Q) = gr(P) + gr(R),$$

$$kgr(Q) - gr(P) = gr(R),$$

$$hgr(P) = kgr(Q) - gr(P) = kgr(P) - gr(P) = (k - 1)gr(P),$$

de modo que $h = k - 1$ y esto es imposible ya que h y k son pares.

Para $a = 1$, $c = 0$, la prueba es análoga.

Si $a = c = 0$ entonces por (11) $e = h$ y $f = k$. Además, por (8) y (9) teniendo en cuenta que $b = d$ y el $gr(P) = gr(Q)$, se concluye que $h = k$ lo cual implica $e = f$. Por otra parte, como $l = 2$ se tiene de (10)

$$1 + R + R^2 = (PQ)^e$$

Con $e > 0$ par, esto es imposible por el lema 2. □

3. Polinomios perfectos impares que son un producto de cuadrados de primos

Aquí se muestran algunos resultados generales sobre *posibles polinomios perfectos impares* $A \in F_2[x]$ que satisfacen ciertas condiciones

Lema 5. *Sean* P *y* $Q \in F_2[x]$ *dos primos distintos del mismo grado* d. *Si* Q *divide* $\sigma(P^2)$ *entonces* P *no divide a* $\sigma(Q^2)$.

Demostración: Supongamos que:

$$\sigma(P^2) = 1 + P + P^2 = QC \tag{12}$$

y

$$\sigma(Q^2) = 1 + Q + Q^2 = PB \tag{13}$$

Como $1 + P + P^2 = 1 + P(P + 1) = QC$, entonces $Q \nmid P + 1$. Por otra parte, usando el hecho de que estamos en característica 2, tenemos $P^3 + 1 = (P + 1)(P^2 + P + 1)$, y de (12) concluimos que:

$$Q \mid P^3 + 1.$$

Luego, se puede afirmar que:

$$Q \mid Q + Q^2 + (P^3 + 1) = 1 + Q + Q^2 + P^3. \tag{14}$$

Reemplazando (13) en (14), vemos que

$$Q \mid PB + P^3 = P(B + P^2)\ ;$$

pero como $Q \nmid P$ obtenemos

$$Q \mid B + P^2; \tag{15}$$

por lo tanto,

$$Q \mid B^2 + BP^2 = B^2 + (BP)P\ . \tag{16}$$

Reemplazando (13) en (16), obtenemos:

$$Q \mid B^2 + P + PQ + PQ^2 = (B^2 + P) + Q(P + PQ)$$

y, en consecuencia,

$$Q \mid B^2 + P\ ; \tag{17}$$

de (15) y (17) se tiene ahora que:

$$Q \mid (B^2 + P) + (B + P^2) = (B^2 + P^2) + (B + P);$$

utilizando el teorema 1 del capítulo 2, se obtiene:

$$Q|\ (B+P)^2+(B+P)=\ (B+P)(B+P+1).$$

Como Q es irreducible de grado d se concluye que:

$$Q|(B+P)\text{ ó }Q|B+P+1;$$

Pero esto es una contradicción ya que por (13) $d=gr(B)$ y se tendría

$$gr(B+P)<d\text{ y }gr(B+P+1)<d.\quad \square$$

Lema 6. *Sea* $P\ \in\ F_2[x]$ *un primo maximal de un polinomio perfecto especial A con* $w(A\ )=m.$. *Entonces existe una única pareja* $(i,j),i,j\in\{1,\dots,m\}$ *tal que:*

a. $p_j\neq P,d_1<d_i<d_j=gr(p_j)=gr(P)=d_m$. *En otras palabras,* p_j *es maximal mientras* p_i *es medial.*
b. $P|p_i^2+p_i+1$ *y* $P|p_j^2+p_j+1$ *así que* $P=p_i+p_j+1$
c. Si $1+p_i+p_i^2=PR$ *entonces* $0<gr(R)<d_i$, *y por consiguiente* $d_m<2d_i$.

Demostración de a. y b. Se puede asumir que: $P=p_m$. Si $p_m^2\mid\sigma(p_i^2)$ con $i<m$, entonces: $2gr(p_m)\leq 2gr(p_i)$ equivalente a: $d_m\leq d_i$. Como d_m es el mayor grado entonces $d_m=d_i$ y en consecuencia p_m^2 y $\sigma(p_i^2)$ son polinomios del mismo grado y como están sobre F_2 necesariamente son iguales, esto es $p_m^2=p_i^2+p_i+1$. Despejando $p_i=p_m^2+p_i^2+1$ y aplicando el teorema 2 se obtiene: $p_i=(p_m+p_i+1)^2$ lo cual es imposible porque p_i es irreducible. Por lo tanto $p_m^2\nmid\sigma(p_i^2)$ con $i<m$, además $p_m^2|A=\sigma(A\ )=\sigma(p_1^2\ )\cdots\sigma(p_m^2\ )$, entonces p_m es factor en exactamente dos $\sigma(p_k^2\ )$ donde $k\in\{i,j\}$ con $i<j<m$ y $d_i\leq d_j$, es decir:

$$p_m|p_i^2+p_i+1,p_m|p_j^2+p_j+1,$$

donde:

$$p_m|(p_i^2+p_i+1)+(p_j^2+p_j+1)=(p_i^2+p_j^2)+p_i+p_j;$$

aplicando el teorema 1 del capítulo 2, se tiene:

$$p_m\big|(p_i+p_j)^2+p_i+p_j=(p_i+p_j)(p_i+p_j+1),$$

y entonces

$$p_m|\ (p_i+p_j)\quad\text{o}\quad p_m|(p_i+p_j+1)\textbf{.}\qquad(18)$$

Así, $d_m \leq d_j$ es decir $d_j = d_{j+1}$=… = d_m.

Si $d_i = d_j$ entonces $p_i + p_j$ y $p_i + p_j + 1$ ambos tendrían menor grado que d_j y como p_m divide a uno de ellos, se tendría una contradicción: $d_m < d_j$. En consecuencia $d_i < d_j$.

Por (18) y como $gr(p_m) = d_m = d_j = gr(p_i + p_j) = gr(p_i + p_j + 1)$ entonces, $p_m = p_i + p_j + 1$ ó $p_m = p_i + p_j$. La segunda opción no puede ser, porque $p_i + p_j$ no es irreducible ya que todos los irreducibles tienen el término independiente 1 (en caso contrario se podría factorizar *x*), pero al sumar p_i y p_j se cancelan los términos independientes. En conclusión

$$p_m = p_i + p_j + 1. \tag{19}$$

Como $d_j = d_m$ es claro que $p_m \neq \sigma(p_j^2)$. Por otra parte, si $p_m = \sigma(p_i^2)$ entonces, por (19),

$$p_i + p_j + 1 = p_i^2 + p_i + 1,$$

de donde

$$p_j = {p_i}^2.$$

Lo cual constituye una contradicción ya que p_j es irreducible. Así, p_m divide estrictamente a $\sigma(p_i^2)$ y $\sigma(p_j^2)$.

Veamos que $d_1 < d_i$.

Supongamos que $d_1 = d_i$. Como $p_m | p_i^2 + p_i + 1$ existe $Q \in F_2[x]$ tal que,

$$p_m Q = p_i^2 + p_i + 1;$$

entonces *Q* divide a *A* y además

$$gr(Q) + gr(p_m) = 2gr(p_i),$$

entonces

$$gr(Q) + d_m = 2d_1$$

de donde

$$gr(Q) = 2d_1 - d_m = d_1 + (d_1 - d_m) < d_1$$

ya que $d_1 < d_m$. Si $Q \neq 1$ tendría un factor primo *H* tal que $gr(H) < d_1$ que también divide a *A;* esto contradice la definición de d_1, y en consecuencia $Q = 1$; pero esto es imposible ya que p_m divide estrictamente $\sigma(p_i^2)$.

Acabamos de ver que:

$$gr(R) = 2d_i - d_m > 0;$$

por consiguiente,

$$d_m < 2d_i.$$

La unicidad de la pareja (*i*, *j*) se deduce del hecho de que el primo maximal *P* aparece exactamente dos veces en $\sigma(A) = A$. □

Corolario 7. *Sea A un polinomio perfecto especial. Entonces, para cada primo maximal P de A y para cada primo minimal Q de A, P no divide a* $\sigma(Q^2)$.

Demostración. El resultado se obtiene de forma inmediata de la demostración del lema 6 al tener en cuenta dos hechos importantes: en primer lugar, *P* divide a exactamente a dos de $\sigma(R^2)$ y $\sigma(S^2)$ para algunos R *y* S factores primos de *A*. En segundo lugar se demuestra que uno de ellos es maximal y el otro medial, quedando así descartada la posibilidad de que *P* divida a $\sigma(Q^2)$ con Q minimal. □

Corolario 8. *Sea A un polinomio perfecto especial. Sea t el número de primos maximales de A, y sea u el número de primos mediales de A. Entonces* $u \geq t \geq 3$.

Demostración. Por el lema 6.a, aparte de *P* hay al menos otro polinomio maximal, es decir, $t \geq 2$. Supongamos que $t = 2$ y que p_m y p_{m-1} sean los dos primos maximales de *A.* Entonces por el lema 6, $p_m | \sigma(p_{m-1}^2)$ y $p_{m-1} | \sigma(p_m^2)$ lo cual contradice el lema 5 de esta sección. Por lo tanto, $t \geq 3$. Supongamos ahora que $u < t$. Entonces por el lema 6 de esta sección y por el principio del palomar, deben existir *P* y *Q* maximales tales que *P* y *Q* dividen a $\sigma(p_k^2)$ para algún p_k primo medial. Entonces $PQ \mid \sigma(p_k^2)$ esto implica que $2d_m \leq 2d_k$ lo cual es imposible ya que $2d_m > 2d_k$. En conclusión $u > t$. □

Corolario 9. *Sea A un polinomio perfecto especial. Con exactamente tres primos maximales P, Q, R. Supongamos que P divide a* $\sigma(Q^2)$. *Entonces, Q divide* $\sigma(R^2)$ *y R divide a* $\sigma(P^2)$. *Además, sean* P_1, Q_1, R_1, *primos mediales divisores de A tales que P divide a* $\sigma(Q_1^2)$, *Q divide a* $\sigma(R_1^2)$, *R divide a* $\sigma(P_1^2)$, *y* $gr(P_1) \leq gr(Q_1) \leq gr(R_1)$, *entonces* $P_1 + Q_1 + R_1 = 1$. *En particular,*

$$gr(P_1) < gr(Q_1) = gr(R_1).$$

Demostración. Por los lemas 6 y 5 de esta sección, se tiene que Q divide a $\sigma(R^2)$ y que R divide a $\sigma(P^2)$; por el lema 6. b:

$$P = Q + Q_1 + 1,$$

$$Q = R + R_1 + 1,$$

$$R = P + P_1 + 1.$$

Sumando las tres igualdades y simplificando se obtiene:

$$P_1 + Q_1 + R_1 = 1$$

Por la igualdad anterior y como se tiene $gr\ (P_1) \leq gr\ (Q_1) \leq gr\ (R_1)$ se eliminan las siguientes posibilidades:

$$gr\ (P_1) = gr\ (Q_1) = gr(R_1) = m \text{ o } gr\ (P_1) \leq gr\ (Q_1) < gr(R_1) = m,$$

porque en ambos casos x^m aparecería en $P_1 + Q_1 + R_1$. Se tiene entonces:

$$gr\ (P_1) < gr\ (Q_1) = gr(R_1). \quad \square$$

Lema 10. *Sea* $P \in F_2[x]$ *un divisor primo de un polinomio perfecto especial A. Si*

$$S = \sigma(P^2) = 1 + P + P^2 \tag{20}$$

es primo entonces

a. S *no es un primo maximal de A.*

Supongamos además, que P es minimal y que S no es primo entonces:

b. $w(S) = 2$*; más precisamente* $S = 1 + P + P^2 = Q_1 Q_2$*, donde* Q_1 *y* Q_2 *son dos primos mimimales distintos de A.*

c. P *no divide a* $\sigma(Q_1^2)\sigma(Q_2^2)$

Demostración. a. Supongamos que S es primo maximal entonces de (20) concluimos que $gr(S) = 2gr(P)$; por lo tanto, P no puede ser maximal. Por otra parte de (20) también concluimos que $S \mid \sigma(P^2)$ y el corolario 7 implica que P no es minimal; por lo tanto, P es medial. Ahora por el lema 6 c., S debe ser un divisor propio de $\sigma(P^2)$ lo cual contradice a (20).

b. Supongamos ahora que P es minimal y que S no es primo. Se puede escribir

$$S = 1 + P + P^2 = \prod_{i=1}^{r} Q_i \qquad (21)$$

Con Q_i divisor primo, donde $r \geq 2$ pues *S* tiene al menos dos factores primos. Por otra parte (21) implica que $2gr(P) = \sum_{i=1}^{r} gr(Q_i)$, además $gr(Q_i) \geq gr(P)$ ya que *P* es minimal, entonces necesariamente $r = 2$ y $gr(Q_1) = gr(Q_2) = gr(P)$. Por otra parte $Q_1 \neq Q_2$ ya que si $Q_1 = Q_2$ se tendría que

$$1 + P + P^2 = (1 + D + D^2)^2 = 1 + D^2 + D^4,$$

donde $P = D^2$, lo cual es imposible ya que *P* es primo.

c. Por a. y por el lema 5, $P \nmid \sigma(Q_1^2)$ y P $\nmid$ $\sigma(Q_2^2)$ por lo tanto $P \nmid \sigma(Q_1^2)\sigma(Q_2^2)$. □

4. Polinomios perfectos especiales *A* con *w(A)* ≥ 10 y $d_1 \geq 30$

Veamos ahora que los polinomios perfectos especiales deben satisfacer las siguientes condiciones:

i) $w(A) \geq 10$
ii) $d_1 \geq 30$

Sea $A \in F_2[x]$ un polinomio perfecto especial. El primer resultado $w(A) \geq 10$ será probado en dos pasos. Primero, el siguiente lema mostrará que $w(A) \geq 8$. En el segundo, se probará que $w(A) \neq 8$.

Lema 11. Sea $A \in F_2[x]$ *un polinomio perfecto especial entonces,* $w(A) \geq 8$.

Demostración. Por el Corolario 8 se puede afirmar que *A* tiene al menos 6 divisores primos, 3 maximales y 3 mediales. El lema 4 garantiza la existencia de al menos 2 primos minimales de *A.* Por consiguiente, $w(A) \geq 8$. □

Lema 12. *No hay polinomios perfectos especiales* $A \in F_2[x]$ *con* $w(A) = 8$.

Demostración. Si *A* tiene más de dos primos minimales, la demostración anterior implica que $w(A) > 8$. Supongamos que $w(A) = 8$; entonces *A* tiene dos primos minimales P_1 y P_2 . Si $\sigma(P_1^2)$ no es primo, el lema 10 implica que $1 + P_1 + P_1^2 = P_1 P_2$, lo cual constituye una contradicción, luego $\sigma(P_1^2)$ es primo. De manera análoga, $\sigma(P_2^2)$ es primo. Esto implica que $\sigma(P_1^2)$ y $\sigma(P_2^2)$ deben pertenecer a $\{P_1, \ldots, P_8\}$ pero no pueden pertenecer a $\{P_1, P_2\}$ por razón de sus grados. Además, por el corolario 8 podemos afirmar que: P_3, P_4 y P_5 son primos mediales y P_6, P_7 y P_8 son primos maximales; entonces, por el corolario 7, $P_j \nmid \sigma(P_i^2)$ para *i* =

1,2 y j = 6, 7, 8. Por consiguiente $\sigma(P_1^2)$ y $\sigma(P_2^2)$ deben pertenecer a $\{P_3, P_4, P_5\}$. El corolario 9 implica que la única posibilidad para los grados es la siguiente:

$$d_1 = d_2 < d_3 < d_4 = d_5 < d_6 = d_7 = d_8. \quad (22)$$

Sin pérdida de generalidad y teniendo en cuenta a (22), podemos afirmar que:

$$P_4 = \sigma(P_1^2), \quad (23)$$

y $P_5 = \sigma(P_2^2)$. Vamos a demostrar que: $\sigma(P_3^2) = P_8P_2$. Asumimos por el lema 6 que P_8 divide a $\sigma(P_3^2)$, es decir, $P_3^2 + P_3 + 1 = P_8M$ para algún polinomio $M \in F_2[x]$, donde los factores primos de M están contenidos en $\{P_1, \dots, P_8\}$; por consiguiente el $gr(M) = 2d_3 - d_8 = d_3 + (d_3 - d_8) < d_3$, de modo que únicamente primos minimales pueden dividir a M. Tomemos P_2 como un divisor de M; entonces $M = P_2N$ para algún $N \in F_2[x]$, donde los factores primos de N están contenidos en $\{P_1, P_2\}$. Por consiguiente el

$$gr(N) = 2d_3 - d_8 - d_2 < d_3 - d_2 < d_2$$

ya que $d_3 < d_4$ y, por (23), $d_4 = 2d_2$. Así $N = 1$, ya que si $N \neq 1$ entonces tendría un factor primo H' tal que $gr(H) < d_2$, que también divide a M, luego habría otro polinomio minimal y esto contradice el hecho de que son dos los primos minimales, esto es un argumento análogo empleado en el lema 6 de esta sección. Con otras palabras, tenemos $\sigma(P_3^2) = P_3^2 + P_3 + 1 = P_8P_2$ lo que implica que:

$$d_8 = 2d_3 - d_2. \quad (24)$$

Por otra parte como $d_3 < 2d_2$ entonces $2d_3 < 4d_2$ y así $2d_3 - d_1 < 4d_2 - d_1 = 3d_1$. O sea, $d_8 < 3d_1$. Además se tiene que:

$$d_1 < d_3 < d_4 = 2d_2$$

y

$$d_8 = 2d_3 - d_1 < 3d_1. \quad (25)$$

Reemplazando (23) en $\sigma(P_4^2) = P_4^2 + P_4 + 1$ se obtiene:

$$\sigma(P_4^2) = (P_1^2 + P_1 + 1)^2 + P_1^2 + P_1 + 1 + 1;$$

por el teorema 1 del capítulo 2 se tiene:

$$\sigma(P_4^2) = P_1^4 + P_1^2 + 1 + P_1^2 + P_1 = P_1^4 + P_1 + 1.$$

Por el lema 6 de esta sección obtenemos:

$$P_1^4 + P_1 + 1 = \sigma(P_4^2) = P_7 F. \quad (26)$$

De manera análoga se puede afirmar que:

$$P_2{}^4 + P_2 + 1 = \sigma(P_5^2) = P_6 B, \quad (27)$$

donde $F, B \in F_2[x]$.

Del lema 6. c, se deduce ahora que F puede tener únicamente a P_2 *o* P_3 como factores primos ya que $gr(F) < d_4$; por lo tanto, los únicos factores de F serían P_1, P_2 *o* P_3, pero de (26) se deduce que P_1 no puede ser factor. De manera análoga B puede tener únicamente P_1 *o* P_3 como factores primos.

Pero de (23), (22) y (25)

$$2d_1 = d_4 < d_7 = d_6 = d_8 < 3d_1. \quad (28)$$

De (26) se puede concluir que:

$$4d_1 = d_7 + gr(F),$$

o sea,

$$d_7 = 4d_1 - gr(F); \quad (29)$$

así reemplazando (29) en (28) se sigue:

$$2d_1 < 4d_1 - gr(F) < 3d_1,$$

Y, por lo tanto,

$$2d_1 > gr(F) > d_1. \quad (30)$$

De (30) se deduce que F no puede ser igual a P_2. De otra parte, si $F = P_2 P_3$ entonces $gr(F) = d_2 + d_3$; por (22) se concluye que: $d_2 + d_3 > 2d_1$ y esto se contradice con (30). En conclusión $F = P_3$.

Análogamente P_1 no aparece como un factor en B, es decir, $B = P_3$. En consecuencia por (26) y (27):

$$\sigma(P_4^2) = P_7 P_3,$$
$$\sigma(P_5^2) = P_6 P_3 \quad (31)$$

Tomando los grados en (31) y teniendo en cuenta (27) se puede afirmar que:

$$d_3 + d_6 = 4d_1. \tag{32}$$

Por otra parte de (24) y (22) tenemos que:

$$d_6 = 2d_3 - d_1. \tag{33}$$

Resolviendo el sistema conformado por (32) y (33) vemos que:

$$d_3 = \frac{5}{3}d_1,\ d_6 = \frac{7}{3}d_1.$$

Por el lema 6 se tiene:

$$\sigma(P_6^2) = P_8K; \tag{34}$$

y por el corolario 9 obtenemos

$$\left.\begin{array}{l}\sigma(P_7^2) = P_6L\\ \sigma(P_8^2) = P_7M\end{array}\right\} \tag{35}$$

donde *K, L, M* $\in F_2[x]$. Por consiguiente:

$$2d_6 = d_8 + gr(K),$$

de donde resulta que

$$2d_6 - d_8 = d_6 = \tfrac{7}{3}d_1.$$

Analizando los grados en el conjunto de igualdades (34) y (35), se tiene:

$$gr(L) = gr(M) = gr(K) = \frac{7}{3}d_1.$$

Los únicos factores primos posibles son, pues,: P_5, P_4, P_2 una vez y P_1 dos veces. Pero todos estos polinomios tienen grados que son múltiplos enteros de d_1 lo cual constituye una contradicción. □

Lema 13. *Sea* $A \in F_2[x]$ *un polinomio perfecto especial. Sea* $P \in F_2[x]$ *un divisor primo de A. Entonces:*

a. P es congruente con 1 modulo $x^2 + x + 1$.
b. $gr(P)$ *es par.*

Demostración. a**.** Por el lema 4, A no tiene como divisor a $Q = x^2 + x + 1$ ya que éste es el único polinomio irreducible de grado dos en $F_2[x]$. Sea $\overline{F_2}$ una clausura algebraica de F_2 y sea $\alpha \in \overline{F_2}$ tal que $\alpha^2 + \alpha + 1 = 0$. Se tiene que $P(\alpha)P(\alpha^2) \neq 0$, ya que si $P(\alpha) = 0$ el lema 1del capítulo 2, implica que $P(\alpha^2) = 0$. El lema 1 del capítulo 2, también implica que α^2 es raíz de Q por lo tanto $Q = (x - \alpha)(x - \alpha^2)$ luego Q divide a P y como ambos son primos entonces $P = Q$ y esto es una contradicción ya que Q no divide a A. Supongamos que $P(\alpha) \in \{\alpha, \alpha^2\}$ esto es, si $P(\alpha) = \alpha$ entonces

$$(1 + P + P^2)(\alpha) = 1 + \alpha + \alpha^2 = 0,$$

luego, α es raíz del polinomio $1 + P + P^2$. El lema 1 del capítulo 2, implica que α^2 también es raíz de $1 + P + P^2$. Y así Q divide $\sigma(A) = A$, ya que, $\sigma(A) = \left(1 + P_1 + {P_1}^2\right) \ldots (1 + P_n + {P_n}^2)$ y esto es una contradicción.

Se sigue que $P(\alpha) = 1 = P(\alpha^2)$. Sea ahora $h(x) = P(x) + 1$ esto implica que $h(\alpha) = P(\alpha) + 1 = 0$ y, por el lema 1 del capítulo 2, $h(\alpha^2) = 0$ y como α^2 y α son raíces de *h,* entonces Q divide a *h* es decir $Q|P + 1$ o sea:

$$P \equiv 1 (mod\ x^2 + x + 1).$$

b. Sea $F_4 = F_2[\alpha]$. Si P permanece primo en $F_4[x]$ entonces de la igualdad $\sigma(A) = A$ se deduce que P divide a algún $\sigma(R^2) = 1 + R + R^2 = (R + \alpha)(R + \alpha^2)$. Luego, P divide a alguno de los factores, asumimos que P divide $R + \alpha$ en F_4. Así, $P(A + B\alpha) = PA + PB\alpha = R + \alpha$ para algunos $A,\ B \in F_2[x]$. Obtenemos así la contradicción $PB = 1$. Por lo tanto P es compuesto en $F_4[x]$, es decir, es de la forma:

$$P = (C + D\alpha)(E + F\alpha^2). \qquad (36)$$

O sea,

$$P = CE + CF\alpha^2 + DE\alpha + DF\alpha^3 = CE + CF\alpha^2 + DE\alpha + DF = CE + CF(1 + \alpha) + DE\alpha + DF = CE + CF + CF\alpha + DE\alpha + DF = CE + CF + \alpha(CF + DE) + DF,$$

donde $CF + DE = 0$, ya que $P \in F_2[x]$; por lo tanto, $CF = DE$ y, en consecuencia, se tienen las siguientes posibilidades:

$$C = D \text{ y } F = E \text{ o } C = E \text{ y } F = D.$$

Si $C = D$ y $F = E$ entonces reemplazando en (36) obtenemos

$$P = C(1 + \alpha)E(1 + \alpha^2) = CE\alpha^3 = CE,$$

y esto es una contradicción ya que *P* es primo en $F_2[x]$. Entonces $C = E$ y $F = D$ y se tiene $P = (C + D\alpha)(C + D\alpha^2) = C^2 + CD + D^2$, para algún *C, D* $\in F_2[x]$ y así $gr(P)$ es par. □

Corolario 14. Sea A $\in$ F_2[x] un polinomio perfecto especial. Sea P $\in$ F_2[x] un divisor primo minimal de A. Entonces P, todos los divisores primos Q de $\sigma(P^2)$, todos los divisores primos R de $\sigma(Q^2)$ y todos los divisores primos de $\sigma(R^2)$ son congruentes con $1(\mathrm{mod}\ x^2 + x + 1)$ y tienen grados pares.

Demostración. Por el lema anterior, *P* es congruente con 1 modulo $x^2 + x + 1$ y $gr(P)$ es par.
Por otro lado, como $A = {P_1}^2 \cdots {P_n}^2 = \sigma(A) = \sigma({P_1}^2) \cdots \sigma({P_n}^2)$, Q, R son primos, $Q \mid \sigma(P^2)$ y $R \mid \sigma(Q^2)$ entonces $Q \mid A$ y $R \mid A$. Luego, $Q = P_i$ y $R = P_j$ donde $i \neq j$ $i, j \in \{1, .., n\}$. En conclusión, por el lema anterior,

$$Q \equiv 1(mod\ x^2 + x + 1), R \equiv 1(mod\ x^2 + x + 1),$$

$gr(Q)$ y $gr(R)$ son pares. □

Teorema 15. *Sea* $A \in F_2[x]$ *un polinomio perfecto especial. Sea* $P \in F_2[x]$ *un divisor primo minimal de A. Entonces*:

a. $w(A) \geq 10$;
b. $d_1 = gr(P) \geq 30$.

Demostración. Por el corolario 8, *A* tiene al menos 6 divisores primos y la demostración del lema 12 muestra que es imposible que hayan solo dos divisores minimales. Por lo tanto, por el lema 4, deben haber al menos 4. Se obtiene $w(A) \geq 6 + 4 = 10$. Probándose así a.

b. Fue obtenido por **Gallardo, L. & O. Rahavandrainy** ejecutando un programa en Maple 6 basado en el corolario 13.Todos los posibles polinomios *P* con grado menor o igual que 28 fueron probados, y la conclusión del corolario siempre fue infringida. □

BIBLIOGRAFÍA

[1]. **Albis, V. S.,** *Lecciones sobre la aritmética de polinomios*. Bogotá, 2009.

[2]. **Brent, R. P. & G. L. Cohen**, *A New Bound for Odd Perfect Numbers*. Math. Comput. **53** (1989), 431-437 & S7-S24.

[3]. **Brent, R. P., G. L. Cohen & H. J. J te Riele**, *Improved Techniques for Lower Bounds for Odd Perfect Numbers*. Math. Comput. **57** (1991), 857-868.

[4]. **Canaday**, **E. F.**, *The sum of the divisors of a polynomial*, Duke Math.Journal **8** (1941), 721 – 737.

[5]. **Casas**, **O. F.,** *Sobre las propiedades analíticas del anillo de polinomios* $F_q[X]$, Lecturas Matemáticas **22** (2001), 11-33.

[6]. **Castro, I. & J. F. Caicedo**, *Temas de teoría de cuerpos, teoría de anillos y números algebraicos I y II*. Bogotá: Universidad Nacional de Colombia, 2005.

[7]. **Euclides**, *Elementos de geometría*. Contenido en **F. Vera**, *Científicos griegos*, vol. 1. Aguilar, Madrid, 1970, 689-980.

[8]. **Gallardo, L. & O. Rahavandrainy**, *Odd perfect polynomials over* F_2, Journal de Théorie des Nombres de Bordeaux **19** (2007), 167–176.

[9]. **Gallardo, L. & O. Rahavandrainy**, *Perfect polynomials over* F_4 *with less than five prime factors*, Portugaliae Mathematica **64** (2007), 21–38.

[10]. **Gallardo, L. & O. Rahavandrainy**, *Perfect polynomials over* F_3, International Journal of Algebra, **2** (2008), 477- 492.

[11]. **Hagis, P. Jr.**, *Outline of a Proof That Every Odd Perfect Number Has at Least Eight Prime Factors.* Math. Comput. **35** (1980), 1027-1032.

[12]. **Hagis, P. Jr. & G. L. Cohen**, *Every Odd Perfect Number Has a Prime Factor Which Exceeds* 10^6. Math. Comput. **67** (1998), 1323-1330.

[13]. **Herstein, I. N.,** *Topics in Algebra*, New York: Addison-Wesley, 1975.

[14]. **Iannucci, D. E**., *The Second Largest Prime Divisor of an Odd Perfect Number Exceeds Ten Thousand*. Math. Comput. **68** (1999), 1749-1760

[15]. **Knopfmacher, J.**, *Abstract Analytic Number Theory*, New York, Dover, 1990.

[16]. **Muskat, J.B.,** *On divisors of odd perfect numbers.* Math. Comput. **20**. 1966.

[17]. **Niven, I. & H. S. Zuckerman**, *An Introduction to the Theory of Numbers*. Wiley: New York, 1991.