Tesis de Posgrado

Caracterización aritmética de los divisores de polinomios con coeficientes enteros

Guersenzvaig, Natalio Héctor

1987

Tesis presentada para obtener el grado de Doctor en Ciencias Matemáticas de la Universidad de Buenos Aires

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

Tema de Tesis

CARACTERIZACION ARITMETICA DE LOS DIVISORES DE POLINOMIOS CON COEFICIENTES ENTEROS

Autor

Natalio Héctor Guersenzvaig

Director de Tesis

Dr. Enzo R. Gentile

Lugar de trabajo:

Universidad Centro de Altos Estudios en Ciencias Exactas (C.A.E.C.E.)
Departamento de Matemática

Tesis presentada para optar al título de Doctor en Matemática

1987

Dedico esta tesis

a la memoria de mis padres

y

a mi esposa e hijo.

Expreso aquí mi reconocimiento a todos aquellos que hicieron posible esta tesis. En particular deseo agradecer:

a mi Director de Tesis, **Dr. Enzo R. Gentile**, cuyas observaciones y sugerencias permitieron mejorar distintas versiones preliminares de esta presentación;

a las autoridades de la **Universidad C.A.E.C.E.**, por permitirme utilizar libremente las instalaciones de su Laboratorio de Computación;

a la **Lic. Norma Pietrocola**, Directora del **Depto. de Matemática** de la Universidad C.A.E.C.E., por su constante estímulo, sin el cual esta tesis no se habría concretado;

a mi ex-alumno, y ahora amigo, **Lic. Luis L. Lewin**, por su importante contribución a la transcripción de la primera versión de este manuscrito;

a mi ex-alumna **Alejandra Santa María**, por su eficiente colaboración en la transcripción de la versión final de este manuscrito;

al **Lic. Daniel O. Vegega**, Jefe de Asistentes del Laboratorio de Computación de la Universidad C.A.E.C.E. y a los Asistentes del mismo, **Pablo L. Pastor**, **Roberto L. Blanco** y **Fernando J. Sciaccaluga**, por su generosa disposición hacia mi persona.

Buenos Aires
Diciembre, 1987

Natalio H. Guersenzvaig

El problema de distinguir números primos de compuestos, y de descomponer los números compuestos en sus factores primos, es uno de los más importantes y útiles de la aritmética.
... La dignidad de la ciencia exige ciertamente que toda contribución a la solución elegante de un problema tan célebre sea celosamente cultivada.

K. F. GAUSS, Disquisitiones Arithmeticae, Art. 329 (1801)

INDICE

INTRODUCCION

En este trabajo consideraremos polinomios en una indeterminada con coeficientes enteros no todos nulos. Estamos interesados en la relación existente entre los divisores de tales polinomios y sus valores en los enteros. Es un hecho bien conocido (Von Schubert, 1793, redescubierto por Kronecker en 1883; véase [1]) que los divisores de un polinomio arbitrario de grado $n \geq 1$, digamos f, pueden hallarse, "vía" polinomios de interpolación de Lagrange, a partir de los divisores de los valores de f en $n + 1$ enteros cualesquiera distintos entre sí. Probaremos que será suficiente considerar el valor de f en un único entero convenientemente elegido. Más precisamente, asociaremos a f un cierto intervalo real acotado y probaremos que sus divisores están en correspondencia biunívoca con sus valores en uno cualquiera de los enteros del complemento del citado intervalo. Probaremos además que estos valores se caracterizan, entre los divisores del valor asumido por f, mediante condiciones aritméticas sencillas. Los divisores de f se obtienen entonces fácilmente, expandiendo sus valores en una adecuada base numérica. Consecuentemente, caracterizaremos los irreducibles y obtendremos nueva información sobre la naturaleza de los enteros representados por estos polinomios. Las mencionadas condiciones aritméticas se definen independientemente de los polinomios y dan origen a un nuevo método para la investigación de la divisibilidad en los enteros. Como aplicación, resolveremos un problema planteado por Leibnitz en 1679 (véase [2]), estableciendo una propiedad característica de los números de Mersenne con exponente primo.

En distintos corolarios proporcionaremos condiciones suficientes de irreducibilidad relacionadas con otras ya conocidas. Entonces, construiremos los polinomios irreducibles a partir de los enteros, complementando y mejorando así un resultado parcial anterior.

Condiciones aritméticas necesarias y suficientes para coprimalidad y separabilidad, ejemplos y otros hechos menores también tienen lugar en el desarrollo que se realiza a continuación; el mismo es autocontenido en lo esencial y de carácter elemental.

1. POLINOMIOS CON COEFICIENTES ENTEROS

En esta sección estableceremos la terminología apropiada y algunos hechos preliminares. En todo lo que sigue consideraremos (sin pérdida de generalidad) polinomios de $Z[X]$ con coeficiente principal positivo. Sean entonces, f y g dos cualesquiera de tales polinomios. Para fijar ideas

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \ , \ a_n > 0 \ , \ a_k = 0 \ ; \ k > n;$$

$$g = c_m X^m + c_{m-1} X^{m-1} + \ldots + c_1 X + c_0 \ , \ c_m > 0 \ , \ c_k = 0 \ ; \ k > m.$$

1.1. Definición. g es divisor de f (g/f) si existe $h \in Z[X]$ tal que $f = gh$.

Cuando g/f, el único polinomio h (entero si $n = 0$) que satisface 1.1, se denomina complemento de g en f y se denota $g^* = g^*(f)$.

1.2. Definición. f es irreducible si se satisfacen:

I) $f \neq 1$;
II) g/f implica $g = 1$ o $g = f$.

Las colecciones de irreducibles y de divisores de f con coeficiente principal positivo se denotan $I(Z[X])$ y $D(f)$, respectivamente. La intersección de estas dos colecciones se denota $I(f)$. Para $k = 0, 1, \ldots, n$ las subcolecciones de $D(f)$ e $I(f)$ formadas por los polinomios de grado k se denotan $D_k(f)$ e $I_k(f)$, respectivamente.

1.3. Definición. f y g son coprimos si h/f y h/g implica $h = 1$.

1.4. Definición. f es separable si h^2/f implica $h = 1$.

Para evitar trivialidades, a partir de ahora supondremos $n \geq 1$. El máximo común divisor de los coeficientes de f se denomina contenido de f y se denota $c(f)$.

1.5. Definición. f es primitivo si $c(f) = 1$.

Es un hecho bien conocido

1.6. Proposición. Sea f primitivo. Entonces

f es separable sii f y f' son coprimos.

El polinomio

$$f_{prim} = f/c(f)$$

se denomina parte primitiva de f.

Se prueba directamente

1.7. Proposición. Se verifican:

i) f_{prim} es primitivo;

ii) f_{prim}/f;

iii) Si g es primitivo y g/f entonces g/f_{prim}.

El resultado siguiente garantiza que podremos restringirnos, cada vez que sea necesario, a los polinomios primitivos y separables de $Z[X]$:

1.8. Proposición. Existe un único $h \in Z[X]$, con coeficiente principal positivo, tal que

i) h es primitivo y separable;
ii) h/f;
iii) Si g es primitivo y separable y g/f entonces g/h.

Prueba. Claramente, el polinomio (parte primitiva y separable de f)

$$(af/(f,f'))_{prim},$$

donde $(f;f')$ es el máximo común divisor mónico de f y f' (obtenido mediante el algoritmo euclideano en $\mathbb{Q}[X]$) y a es el mínimo común múltiplo de los denominadores de los coeficientes no nulos de $f/(f;f')$ (supuesto que dichos coeficientes se expresan como cociente de enteros coprimos entre sí), es el único polinomio de $\mathbb{Z}[X]$ con coeficiente principal positivo, que verifica las condiciones exigidas.∎

La resultante de f y g es el número real (ciertamente entero)

$$res(f,g) = a_n^m g(z_1)g(z_2)\ldots g(z_n),$$

donde z_k; $k = 1, 2, \ldots, n$ son las n raíces complejas de f.

Obviamente se tiene

1.9. Proposición. Sea f primitivo. Entonces

$$f \text{ y } g \text{ son coprimos sii } res(f,g) \neq 0.$$

En consecuencia

1.10. Corolario. Sea f primitivo. Entonces

$$f \text{ es separable sii } res(f,f') \neq 0.$$

Por otra parte se prueba (véase [3])

1.11. Proposición. Sea $m \geq 1$. Existen únicos f_0, $g_0 \in \mathbb{Z}[X]\setminus\{0\}$ tales que

i) $grado(f_0) < n$, $grado(g_0) < m$;

ii) $res(f,g) = g_0 f + f_0 g$.

Consideramos ahora la matriz de Sylvester de f y g (cuadrada de orden $n + m$), definida

$$S(f,g) = \left\| \begin{matrix} a_n a_{n-1} \ldots a_{n-m+1} \ldots a_0 \ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots a_n a_{n-1} \ldots a_{n-m+1} \ldots a_0 \\ c_m c_{m-1} \ldots c_{m-n+1} \ldots c_0 \ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots c_m c_{m-1} \ldots c_{m-n+1} \ldots c_0 \end{matrix} \right\|.$$

Es un hecho

1.12. **Proposición.** res(f,g) = Det(S(f,g)).

Manipulando S(f,f′) obtenemos la matriz (cuadrada de orden 2n - 1)

$$S(f) = \begin{vmatrix} n & 1 & \cdots & \cdots & \cdots \\ (n-1)a_{n-1} & a_{n-1} & na_n & a_n & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 2a_2 & a_2 & \cdots & \cdots & \cdots \\ 1a_1 & a_1 & 2a_2 & a_2 & \cdots \\ \cdots & \cdots & \cdots & a_0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & a_0 \end{vmatrix}.$$

El entero

$$disc(f) = Det(S(f)).$$

se denomina discriminante de f.

Es bien conocido el hecho siguiente:

1.13. **Proposición.** $res(f,f') = (-1)^{n(n-1)/2} a_n disc(f)$.

Con q denotamos un entero cualquiera. Utilizaremos el resultado que sigue:

1.14. **Proposición.** Sea g/f. Suponemos f separable y res(f,f′)/q. Sea f(0) separable. Entonces

$$g(q) \text{ coprimo con } g^*(q).$$

Prueba. Sea d el máximo común divisor de g(q) y g*(q). Dado que f = gg* tenemos

$$f'(q) = g^*(q)g'(q) + g(q)g^{*\prime}(q).$$

En consecuencia

$$d/f'(q).$$

Por 1.11 ocurre

$$d/res(f,f').$$

Luego d/q. Esto implica

$$d/g(0)\ ,\ d/g^*(0).$$

Entonces

$$d^2/f(0).$$

Dado que f(0) es separable resulta

$$d = 1.\#$$

Los enteros representados por f son los valores f(k); k ∈ Z. El máximo común divisor de tales enteros se denota d(f).

1.15. Definición. f es totalmente primitivo si d(f) = 1.

1.16. Definición. f es totalmente irreducible si se satisfacen:

I) f es irreducible;
II) f es totalmente primitivo.

Para calcular d(f) utilizaremos el resultado siguiente:

1.17. Proposición. d(f) es el máximo común divisor de f(k) ; k = 0, 1, ... , .

Prueba. Sea d el máximo común divisor de f(k); k = 0, 1, 2, ... , n. Obviamente

$$d(f)/d.$$

Sea x un entero arbitrario. Consideramos para k = 0, 1, ... , el número combinatorio generalizado

$$\binom{x}{k} = x(x-1)\ldots(x-k+1)/k!.$$

Es un hecho aritmético elemental

$$x \in Z \text{ implica } \binom{x}{k} \in Z \; ; \; k = 0, 1, \ldots ,.$$

Definimos ahora (variaciones de f en 0)

$$\underline{\Delta} f(0) = \underline{\Delta}^1 f(0) = f(1) - f(0),$$

$$\underline{\Delta}^{k+1} f(0) = \underline{\Delta}(\underline{\Delta}^k f(0)); \; k = 1, 2, \ldots .$$

Convenimos

$$\underline{\Delta}^0 f(0) = f(0).$$

Sea k entero no negativo. Razonando inductivamente obtenemos

$$\underline{\Delta}^k f(0) = \binom{k}{0} f(k) - \binom{k}{1} f(k-1) + \ldots + (-1)^k \binom{k}{k} f(0).$$

Entonces, es fácil ver

$$d/\underline{\Delta}^k f(0).$$

Por otra parte, es un hecho bien conocido (Newton)

$$f(x) = \binom{x}{0} \underline{\Delta}^0 f(0) + \binom{x}{1} \underline{\Delta}^1 f(0) + \ldots + \binom{x}{n} \underline{\Delta}^n f(0).$$

Luego

$$d/f(x).$$

Entonces

$$d/d(f).$$

En consecuencia

$$d = d(f).\#$$

El polinomio

$$f_q = f(X+q) = (f^{(n)}(q)/n!)X^n + \ldots + (f'(q)/1!)X + f(q)$$

se denomina q-traslación de f.

1.18. Nota. Las traslaciones

$$T_q : h \dashrightarrow T_q(h) = h_q,$$

constituyen el grupo de automorfismos del monoide formado por los polinomios de Z[X] con coeficiente principal positivo. Luego preservan primitividad, primitividad total, separabilidad, irreducibilidad e irreducibilidad total.

Observando que $d(f_q) = d(f)$, de 1.17 se deduce (Hensel; véase [2])

1.19. Corolario. d(f) es el máximo común divisor de f(q+k) ; k = 0, 1, ... , .

Por otra parte, se prueba fácilmente

1.20. Proposición. Se verifican:

i) $D(f) = (h(X-q) : h \in D(f_q))$;

ii) $I(f) = (h(X-q) : h \in I(f_q))$.

Estableceremos ahora algunas acotaciones relativas a los coeficientes y raíces de los polinomios de Z[X] (información adicional puede hallarse en [4], [5], [6] y [7]).

Para k = -1, 0, 1, ... , n-1 definimos (| | = módulo)

$$r_k(f) = \mathrm{Sup}_{i=0,\,1,\,\ldots\,,\,n-k-1}\,|a_i|.$$

En primer lugar y en relación con los coeficientes de f_q, tenemos

1.21. Proposición. $r_{-1}(f_q) \leq (1 + |q|)^n r_{-1}(f)$.

Prueba. Para $k = 0, 1, \dots, n$ ocurre

$$f^{(k)}(q)/k! = \binom{k}{0}a_k + \binom{k+1}{1}a_{k+1}q + \dots + \binom{n}{n-k}a_n q^{n-k}.$$

Luego

$$|f^{(k)}(q)/k!| \leq \left(\binom{n}{0} + \binom{n}{1}|q| + \dots + \binom{n}{n}|q|^n\right) r_{-1}(f).$$

Esto es

$$|f^{(k)}(q)/k!| \leq (1 + |q|)^n r_{-1}(f).\#$$

Con w denotamos un complejo arbitrario. Se prueba directamente (Re = parte real)

1.22. **Lema.** Sea $w \neq 0$. Para $k = 0, 1, \dots, n-1$ se verifican:

i) $|f(w)/w^n| > |a_n + a_{n-1}/w + \dots + a_{n-k}/w^k| - |a_{n-k+1}|/|w|^{k+1} - \dots - |a_0|/|w|$;

ii) $|a_{n-k-1}|/|w|^{k+1} + \dots + |a_0|/|w|^n < r_k(f)/(|w|^{k+1} - |w|^k)$;

iii) $|f(w)/w^n| > \mathrm{Re}(a_n + a_{n-1}/w + \dots + a_{n-k}/w^k) - r_k(f)/(|\ |^{k+1} - |w|^k)$.

Es un hecho bien conocido (Cauchy)

1.23. **Proposición.** Sea r real positivo tal que

$$|a_n| > |a_{n-1}|/r + \dots + |a_1|/r^{n-1} + |a_0|/r^n.$$

Entonces las raíces de f se encuentran en el disco $|z| < r$.

Prueba. Sea w raíz no nula de f. Por 1.22 i), con $k = 0$, resulta

$$0 = |f(w)/w^n| \geq |a_n| - |a_{n-1}|/|w| - \dots - |a_1|/|w|^{n-1} - |a_0|/|w|^n.$$

Observamos ahora que la función

$$x \dashrightarrow |a_{n-1}|/x + |a_{n-2}|/x^2 + \dots + |a_0|/x^n$$

es una "permutación" decreciente de los reales positivos. Entonces, por nuestra hipótesis, la desigualdad previa implica

$$|w| < r.\#$$

Por 1.22 i) y ii), con $r = 1 + r_0(f)$, obtenemos de 1.23 la cota siguiente (también debida a Cauchy)

1.24. **Corolario.** Las raíces de f se encuentran en el disco $|\ | < 1 + r_0(f)/a_n$.

En este punto es conveniente la siguiente definición:

1.25. Definición. f es no negativo (positivo) si satisface:

$$a_k \geq 0 \ (a_k > 0;\ \text{respectivamente});\ k = 0, 1, \ldots , \ .$$

Podemos establecer entonces

1.26. Proposición. Sea f no negativo. Entonces sus raíces con parte real positiva se encuentran en el disco

$$|\ | < (1 + (1 + 4r_1(f)/a_n)^{1/2})/2.$$

Prueba. Sea w raíz de f con parte real positiva. Entonces

$$\mathrm{Re}(1/w) = \mathrm{Re}(w)/|\ |^2 > 0.$$

Luego

$$\mathrm{Re}(a_n + a_{n-1}/w) \geq a_n.$$

Por 1.22 iii), con k = 1, resulta

$$|w|^2 - |w| - r_1(f)/a_n < 0.$$

Resolviendo esta inecuación obtenemos

$$|\ | < (1 + (1 + 4r_1(f)/a_n)^{1/2})/2.\#$$

Cuando f es no negativo $r_{-1}(f)$ se denomina radio de f y se denota r(f). Esto es

$$r(f) = \mathrm{Sup}_{k=0,\ 1,\ \ldots} a_k.$$

Dado que $r_1(f) \leq r_{-1}(f)$ se tiene

1.27. Corolario. Sea f no negativo. Entonces sus raíces con parte real positiva se encuentran en el disco

$$|z| < (1 + (1 + 4r(f))^{1/2})/2.$$

En consecuencia

1.28. Corolario. Sea f no negativo. Entonces sus raíces se encuentran en el semiplano

$$\mathrm{Re}(z) < (1/4 + r(f))^{1/2} + 1/2.$$

Tendremos oportunidad de utilizar la siguiente mejora de 1.28:

1.29. Proposición. Sea f no negativo. Entonces sus raíces se encuentran en el semiplano

$$Re(z) < (1 + r(f))^{1/2}.$$

Prueba. Podemos asumir $a_0 > 0$ y $n \geq 3$. Sea w tal que

$$f(w) = 0 \ , \ Re(w) > 0.$$

En primer lugar suponemos

$$a_{n-1} = a_{n-2} = a_{n-3} = 0.$$

Entonces, consideramos el polinomio

$$h = a_n x^n - a_{n-1} x^{n-1} - a_{n-2} x^{n-2} - \ldots - a_0.$$

Evaluando en $(1+r(f))^{1/2}$ obtenemos

$$h((1+r(f))^{1/2}) > (1+r(f))^{n/2} - (1+r(f))^{n/2-1} - (1+r(f))^{n/2-3} - (1+r(f))^{1/2} - 1.$$

De la desigualdad precedente deducimos

$$h((1+r(f))^{1/2}) > (1+r(f))^{n/2-3}((1+r(f))^3 - (1+r(f))-1) > 0.$$

La conclusión sigue entonces de $Re(w) \leq |w|$, pues 1.23 implica

$$|w| < (1 + r(f))^{1/2}.$$

Suponemos ahora a_{n-1}, a_{n-2} y a_{n-3} no todos nulos. Sea además

$$Re(w) \geq (1 + r(f))^{1/2}.$$

Dado que $f(w) = 0$, por 1.27 ocurre

$$|w| \leq (1 + (1 + 4\, r(f))^{1/2})/2.$$

De 1.22 i) y iii), con $k = 3$, obtenemos

$$|f(w)/w^n| > Re(a_n + a_{n-1}/w + a_{n-2}/w^2 + a_{n-3}/w^3) - r(f)/(|w|^4 - |w|^3).$$

Calculando directamente resulta

$$Re(1/w) > Re(1/w^2) > Re(1/w^3) = Re(w)\,(4\, Re^2(w) - 3\,|w|^2)/|w|^6,$$

$$Re(a_n + a_{n-1}/w + a_{n-2}/w^2 + a_{n-3}/w^3) \geq Re(1 + 1/w^3) \geq r(f)/(|w|^4 - |w|^3).$$

Entonces, tenemos la contradicción

$$|f(w)/w^n| > 0,$$

con lo cual la demostración está completa.∎

2. POLINOMIOS ESTABLES Y CUASI-ESTABLES

En esta sección consideramos polinomios bien conocidos (las referencias más importantes son [4] y [8]).

2.1. Definición. f es estable si sus raíces se encuentran en el semiplano $Re(z) < 0$.

El carácter de f, en lo concerniente a estabilidad, puede determinarse considerando, para $k = 1, 2, \ldots, n$, las matrices siguientes (cuadradas de orden k):

$$H_k(f) = \begin{vmatrix} a_1 & a_0 & \cdots & & \\ a_3 & a_2 & a_1 & a_0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{2k-1} & a_{2k-2} & a_{2k-3} & \cdots & a_k \end{vmatrix}$$

Entonces, se tiene (Routh-Hurwitz-Lienard-Chipart)

2.2. Proposición. Son equivalentes:

i) f es estable;

ii) I) f es positivo

II)Los determinantes $Det(H_{n-2k+1}(f))$; $1 \leq k \leq n/2$, son positivos.

Con mayor generalidad consideramos los polinomios siguientes:

2.3. Definición. f es cuasi-estable si sus raíces se encuentran en el semiplano

$$Re(z) \leq 0.$$

Resulta trivialmente

2.4. Proposición. Si f es cuasi-estable (estable) y g/f entonces g es cuasi-estable (estable, respectivamente).

Observando los signos de los coeficientes de los factores irreducibles de f en R[X] (ciertamente de grado ≤ 2), deducimos de 2.4 el hecho siguiente:

2.5. Proposición. Si f es cuasi-estable (estable) y g/f entonces g, g^* son no negativos (positivos, respectivamente).

Por otra parte se prueba directamente

2.6. Proposición. f_q es cuasi-estable (estable) sii las raíces de f se encuentran en el semiplano $Re(z) \leq q$ ($Re(z) < q$, respectivamente).

2.7. Corolario. Si las raíces de f se encuentran en el semiplano

$$Re(z) < q + 1/2$$

entonces

$$|f(q)| < f(q+1).$$

Prueba. Ciertamente, 2.5 y 2.6 siguen vigentes cuando q y los coeficientes de f son reales cualesquiera. Luego $f_{q+1/2}$ tiene positivos sus coeficientes no nulos. Dado que $n > 1$ resulta

$$|f(q)| = |f_{q+1/2}(-1/2)| < |f_{q+1/2}(1/2)| = f(q+1).\#$$

Por 1.24, 2.4, 2.5 y 2.6 podemos restringirnos a los polinomios cuasi-estables no negativos. Con mayor generalidad consideraremos los polinomios no negativos (un desarrollo semejante tiene lugar utilizando polinomios positivos). Supondremos entonces, salvo especificación en contrario, f y g no negativos.

3. POLINOMIOS NO NEGATIVOS

La colección de enteros no negativos se denota $Z^{\langle+\rangle}$. Las definiciones básicas relativas a la divisibilidad en $Z^{\langle+\rangle}[X]\backslash\{0\}$ son las siguientes:

3.1. Definición. g es $\langle+\rangle$-divisor de f ($g/_{\langle+\rangle}f$) si se satisfacen:

I) g/f;
II) $g^*(f)$ es no negativo.

3.2. Nota. En términos probabilísticos, expresar f como producto de polinomios no negativos equivale a expresar una cierta variable aleatoria X_f, con función de probabilidad $p_f(k) = Pr(X_f = k) = a_k/f(1)$; $k = 0, 1, \ldots, n$, como suma de variables aleatorias con funciones de probabilidad racionales independientes entre sí.

3.3. Definición. f es $\langle+\rangle$-irreducible si se satisfacen:

I) $f \neq 1$;
II) $g/_{\langle+\rangle}f$ implica $g = 1$ o $g = f$.

3.4. Nota. Ciertamente, las ⟨+⟩-factorizaciones de los polinomios no negativos siempre existen, pero no son necesariamente únicas. Por ejemplo, los polinomios

$$g = X + 2\ ,\ g^* = X^3 + 2X + 3\ ,\ h = X + 1 \quad y \quad h^* = X^3 + X^2 + X + 6$$

son ⟨+⟩-irreducibles y $gg^* = hh^*$.

Las colecciones de ⟨+⟩-irreducibles y de ⟨+⟩-divisores de f se denotan $I(Z^{\langle+\rangle}[X])$ y $D^{\langle+\rangle}(f)$, respectivamente. La intersección de estas colecciones se denota $I^{\langle+\rangle}(f)$. Para $k = 0, 1, \ldots, n$ las subcolecciones de $D^{\langle+\rangle}(f)$ e $I^{\langle+\rangle}(f)$ formadas por los polinomios de grado k se denotan $D_k^{\langle+\rangle}(f)$ e $I_k^{\langle+\rangle}(f)$, respectivamente.

3.5. Definición. f es totalmente ⟨+⟩-irreducible si se satisfacen:

I) f es ⟨+⟩-irreducible;
II) f es totalmente primitivo.

3.6. Definición. f y g son ⟨+⟩-coprimos si $h/_{\langle+\rangle}f$ y $h/_{\langle+\rangle}g$ implica $h = 1$.

3.7. Definición. f es ⟨+⟩-separable si $h^2/_{\langle+\rangle}f$ implica $h = 1$.

Mostraremos ahora que podemos restringirnos a polinomios no negativos con coeficientes acotados por un valor prefijado. En primer lugar tenemos

3.8. Proposición. Suponemos $g/_{\langle+\rangle}f$. Sean c_k^* ; $k = 0, 1, \ldots$, los coeficientes de g^*. Entonces

$$a_{i+j} \geq c_i c_j^* \ ;\ i, j = 0, 1, \ldots .$$

Prueba. La no negatividad de g y g^* implica

$$a_{i+j} = c_{i+j}c_0^* + \ldots + c_i c_j^* + \ldots + c_0 c_{i+j}^* \geq c_i c_j^* \ ;\ i, j = 0, 1, \ldots .\#$$

En consecuencia

3.9. Corolario. Si $g/_{\langle+\rangle}f$ entonces $r(g)r(g^*) \leq r(f)$.

Entonces, resulta

3.10. **Corolario.** Sea $f \neq 1$. Entonces f es $\langle + \rangle$-irreducible o bien f tiene un $\langle + \rangle$-divisor propio h (esto es, distinto de 1 y de f) verificando cualquiera de las afirmaciones siguientes:

I) $\text{grado}(h) \leq n/2$;

II) $r(h) < r(f)^{1/2}$.

Además, si h satisface I) y tiene grado mínimo entre tales polinomios o h satisface II) y tiene radio mínimo entre los polinomios que satisfacen II) entonces h es $\langle + \rangle$-irreducible.

Asimismo, de 3.9 se deduce

3.11. **Corolario.** Si $g/_{\langle + \rangle} f$ entonces $r(g) \leq r(f)$.

3.12. **Nota.** En general, 3.11 no se puede mejorar. Por ejemplo, los polinomios

$$f = X^3 + 6X^2 + X + 6 \quad \text{y} \quad g = X^2 + 6$$

verifican

$$g/_{\langle + \rangle} f \quad \text{y} \quad r(g) = r(f).$$

Además, 3.11 se deduce tambien del hecho siguiente (corolario de 3.8 con $j = 0$):

$$\text{si } a_0 > 0 \text{ entonces } g/_{\langle + \rangle} f \text{ implica } c_i \leq a_i \; ; \; i = 0, 1, \ldots, m.$$

Por otra parte, si f, g, g^* son positivos y $g \neq f$, se verifican las acotaciones siguientes (cotas inmejorables para polinomios de $\mathbb{C}[X]$ pueden hallarse en [9]):

i) Sea $a_k(m) = \text{Inf}_{i=0, \ldots, n-m} \text{Inf}\{a_{k+1}, a_{n-m+k-i}\}$; $k = 0, 1, \ldots, m$. Entonces

$$c_0 \leq a_0(m), \; c_k < a_k(m); \; k = 1, 2, \ldots, m-1, \; c_m \leq a_m(m);$$

iii) Si $m \leq n/2$ entonces $g(1) < \text{Inf}\{a_m, a_{n-m}\}$.

En lo que sigue, p denota un entero arbitrario ≥ 2.

3.13. **Corolario.** Si $r(f) < p$ entonces $g/_{\langle + \rangle} f$ implica $r(g) < p$.

4. P-POLINOMIOS

Por 3.13 conviene considerar los polinomios siguientes:

4.1. **Definición.** f es p-polinomio si $r(f) < p$.

La colección de p-polinomios se denota $\mathbb{Z}^{\langle p \rangle}[X]$. Estableceremos entonces condiciones necesarias y suficientes para que $f \in \mathbb{Z}^{\langle p \rangle}[X]$.

4.2. Proposición. Son equivalentes ([ ] = parte entera):

i) $r(f) < p$;

ii) $a_k = [f(p)/p^k] - p[f(p)/p^{k+1}]$; $k = 0, 1, \ldots$,.

Prueba. Suponemos i). Entonces ii) sigue de

$$[f(p)/p^k] = a_k + a_{k+1}p + \ldots + a_n p^{n-k} \; ; \; k = 0, 1, \ldots .$$

Recíprocamente, suponemos ii). Sea k entero no negativo. Ciertamente

$$a_k = [f(p)/p^k] - p[[f(p)/p^k]/p].$$

Entonces i) sigue pues a_k es el resto de dividir $[f(p)/p^k]$ por p.#

Alternativamente, reformulamos 4.2 de la manera siguiente:

4.3. Proposición. Son equivalentes:

i) $r(f) < p$;

ii) $f = f(p) + (X - p)([f(p)/p] + [f(p)/p^2]X + \ldots + [f(p)/p^n]X^{n-1})$.

Entonces, elementales y bien conocidas condiciones necesarias y suficientes para la igualdad de p-polinomios pueden establecerse como sigue:

4.4. Corolario. Sea $\mathrm{Sup}\{r(f), r(g)\} < p$. Son equivalentes:

i) $f = g$;
ii) $f(p) = g(p)$.

Podemos ahora reformular 4.4 de la manera siguiente:

4.5. Corolario. Sea $r(f) < p$. Son equivalentes:

i) $f = g$;
ii) $f(p) = g(p)$ y $r(g) < p$.

Tiene interés propio e inesperadas consecuencias (además de 4.5) el hecho que sigue:

4.6. Proposición. Suponemos $r(f) < p$. Sea $h \in Z[X]$ tal que

$$f = g + (X - p)h.$$

Se verifican:

i) h es no negativo;
ii) $h = 0$ o $r(h) < r(g)/(p - 1)$ $(\leq r(g)/r(f))$.

Prueba. Suponemos h no nulo. Sean b_k; k = 0,1, ... , los coeficientes de h. Convenimos

$$b_{-1} = 0.$$

Ciertamente

$$a_k + pb_k = c_k + b_{k-1} \; ; \; k = 0, 1, \ldots .$$

Con k = 0 resulta

$$a_0 + pb_0 = c_0.$$

La hipótesis r(f) < p implica

$$0 \leq b_0 = (c_0 - a_0)/p \leq c_0/p.$$

Afirmamos

$$0 \leq b_k \leq c_k/p + \ldots + c_1/p^k + c_0/p^{k+1} \; , \; k = 0, 1, \ldots ,.$$

Entonces, suponemos que estas desigualdades se verifican para k < s. Sea k = s. Luego

$$a_s + pb_s = c_s + b_{s-1}.$$

En consecuencia

$$0 \leq b_s = (c_s + q_{s-1} - a_s)/p \leq c_s/p + c_{s-1}/p^2 + \ldots + c_0/p^{s+1}.$$

Puesto que para k = 0, 1, ... , tenemos

$$c_k/p + \ldots + c_1/p^k + c_0/p^{k+1} < r(g)(1/p + 1/p^2 + \ldots) = r(g)/(p - 1),$$

la demostración está completa.#

Ciertamente los polinomios de $Z^{\langle + \rangle}[X]\backslash\{0\}$ no poseen raíces positivas. Deducimos entonces de 4.6

4.7. Corolario. Suponemos r(f) < p. Sea w real positivo, w ≠ p. Son equivalentes:

i) f = g;
ii) f(p) = g(p) y f(w) = g(w).

En particular ocurre

4.8. Corolario. Son equivalentes:

i) f = g;
ii) f(p) = g(p) y f(1) = g(1).

Derivando sucesivamente y evaluando en ambos miembros de f = g + (X - p)h probamos

4.9. Corolario. Sean w real $\geq p$ y k entero positivo arbitrario. Convenimos

$$f^{(-1)}(0) = g^{(-1)}(0) = 0.$$

Son equivalentes:

i) $f = g$;

ii) $f(p) = g(p)$, $f^{(j)}(0) = g^{(j)}(0)$; $j = -1, \ldots, k-2$ y $f^{(k)}(w) = g^{(k)}(w)$.

Con $k = 1$ obtenemos

4.10. Corolario. Son equivalentes:

i) $f = g$;
ii) $f(p) = g(p)$ y $f'(p) = g'(p)$.

5. EVALUACIONES

Aprovecharemos ahora lo hecho en la sección precedente, para representar en Z los $\langle + \rangle$-divisores de los p-polinomios.

La aplicación

$$\langle\langle q \rangle\rangle : Z[X] \text{ -----> } Z : h \text{ -----> } \langle\langle q \rangle\rangle(h) = h(q)$$

se denomina q-evaluación.

Son hechos elementales

5.1. Proposición. Se verifican:

i) $\langle\langle q \rangle\rangle$ es el único morfismo de anillos entre $Z[X]$ y Z que satisface:

$$\langle\langle q \rangle\rangle(X) = q;$$

ii) $\langle\langle q \rangle\rangle$ es suryectiva;

iii) El núcleo de $\langle\langle q \rangle\rangle$ es el ideal de $Z[X]$ generado por $X - q$.

De 4.4 se deduce

5.2. Corolario. La restricción

$$\langle\langle p \rangle\rangle : Z^{\langle p \rangle}[X] \setminus \{0\} \text{ -----> } Z^{\langle + \rangle} \setminus \{0\}$$

es inyectiva.

Por 3.13 y 5.2 se tiene

5.3. **Proposición.** La restricción

$$\langle\langle p\rangle\rangle : D^{\langle+\rangle}(f) \longrightarrow D^{\langle+\rangle}(f(p))$$

es inyectiva.

6. P-EXPANSIONES Y P-POLINOMIOS DE ENTEROS

En virtud de 5.3 es conveniente un lenguaje más aritmético. Con a y c denotamos enteros positivos cualesquiera.

Los números

$$a_k(p) = [a/p^k] - p[a/p^{k+1}] \; ; \; k = 0, 1, \ldots ,$$

se denominan p-coeficientes de a. El entero

$$n_p = n_p(a) = \mathrm{Sup}\{k \in Z : p^k \leq a\}$$

se llama p-grado de a. El entero positivo

$$r_p(a) = \mathrm{Sup}_{k=0, 1, \ldots} a_k(p)$$

se denomina p-radio de a. El término

$$(a_{n_p}(p)\ldots a_1(p)a_0(p))_p = a_{n_p}(p)p^{n_p} + \ldots + a_1(p)p + a_0(p)$$

se denomina p-expansión de a. El polinomio

$$a_{\langle p\rangle} = a_{n_p}(p)X^{n_p} + \ldots + a_1(p)X + a_0(p)$$

se denomina p-polinomio de a.

Se prueba directamente ($\log_p$ = logaritmo en base p)

6.1. **Proposición.** $n_p(a) = [\log_p a]$.

Dado que para $k = 0, 1, \ldots$ $a_k(p)$ es el resto de dividir $[a/p^{k+1}]$ por p, se tiene

6.2. **Proposición.** $r_p(a) < p$.

De las definiciones anteriores se deduce

6.3. **Corolario.** $a_{\langle p\rangle} = a + (X - p)([a/p] + [a/p^2]X + \ldots + [a/p^{n_p}]X^{n_p-1})$.

Siendo $r(a_{\langle p\rangle}) = r_p(a)$, por 4.2 resulta

6.4. Proposición. $a_{\langle p\rangle}$ es el único p-polinomio que satisface $a_{\langle p\rangle}(p) = a$.

Claramente, 6.4 equivale al resultado siguiente (existencia y unicidad de las p-expansiones):

6.5. Proposición. Los p-coeficientes y el p-grado de a son los únicos enteros que satisfacen:

I) $0 \leq a_k(p) < p$; $k = 0, 1, \ldots, a_{n_p} > 0$;

II) $a = (a_{n_p}(p)\ldots a_1(p)a_0(p))_p$.

La aplicación

$$\langle p\rangle : Z^{(+)}\backslash\{0\} \text{ -----> } Z^{(+)}[X]\backslash\{0\} : b \text{ -----> } \langle p\rangle(b) = b_{\langle p\rangle}$$

se denomina p-polinomio.

Por 5.2, 6.2 y 6.4 se tiene

6.6. Corolario. Las restricciones

$$\langle\langle p\rangle\rangle : Z^{\langle p\rangle}[X]\backslash\{0\} \text{ -----> } Z^{(+)}\backslash\{0\},$$

$$\langle p\rangle : Z^{(+)}\backslash\{0\} \text{ -----> } Z^{\langle p\rangle}[X]\backslash\{0\},$$

son biyectivas e inversas entre sí.

Asimismo, 5.3 puede reformularse como sigue:

6.7. Proposición. La restricción

$$\langle\langle p\rangle\rangle : D^{(+)}(a_{\langle p\rangle}) \text{ -----> } D^{(+)}(a)$$

es inyectiva.

Con mayor generalidad, se prueba directamente

6.8. Proposición. Suponemos $q \geq 2$. Sea $a \geq c$. Entonces

$$a_{\langle p\rangle} = c_{\langle q\rangle} \text{ sii } p \geq q \text{ y } a = c_{\langle q\rangle}(p).$$

7. (+)-DIVISORES DE P-POLINOMIOS DE ENTEROS

Por 6.7, nuestra tarea consiste en determinar cuáles de las p-expansiones de los

divisores positivos de a son p-evaluaciones de $\langle+\rangle$-divisores de $a_{\langle p\rangle}$. En esta sección estableceremos condiciones necesarias y suficientes para que $c_{\langle p\rangle}$ sea $\langle+\rangle$-divisor de $a_{\langle p\rangle}$.

7.1. **Proposición.** Sea c/a. Son equivalentes:

i) $c_{\langle p\rangle}/_{\langle+\rangle}a_{\langle p\rangle}$;

ii) $c_{\langle p\rangle}/a_{\langle p\rangle}$ y $(c_{\langle p\rangle})^* = c^*_{\langle p\rangle}$;

iii) $a_{\langle p\rangle} = c_{\langle p\rangle}c^*_{\langle p\rangle}$.

Prueba. Las implicaciones ii) ----> iii) y iii) ----> i) son triviales. Suponemos i). Entonces, tenemos

$$(c_{\langle p\rangle})^* \text{ no negativo y } a_{\langle p\rangle} = c_{\langle p\rangle}(c_{\langle p\rangle})^*.$$

Ahora utilizamos 6.4. Evaluando en p resulta $a = cc_{\langle p\rangle}{}^*(p)$, equivalente a

$$c^* = (c_{\langle p\rangle})^*(p).$$

Esto es

$$c^*_{\langle p\rangle}(p) = (c_{\langle p\rangle})^*(p).$$

Puesto que $c^*_{\langle p\rangle}$ y $(c_{\langle p\rangle})^*$ son p-polinomios obtenemos

$$c^*_{\langle p\rangle} = (c_{\langle p\rangle})^*.\#$$

8. $\langle P\rangle$-DIVISIBILIDAD Y $\langle P\rangle$-IRREDUCIBILIDAD

Por 7.1 son oportunas las definiciones siguientes:

8.1. **Definición.** c es $\langle p\rangle$-divisor de a ($c/_{\langle p\rangle}a$) si se satisfacen:

I) c/a;

II) $a_k(p) = c_k(p)c_0^*(p) + c_{k-1}(p)c_1^*(p) + \ldots + c_0(p)c_k^*(p)$; k = 0, 1, ...

La condición II) expresa que el producto de las p-expansiones de c y c* se realiza como si dichas expansiones fuesen polinomios en la "indeterminada" p, esto es, sin transporte de dígitos (véase [10]).

8.2. **Ejemplo.** Ciertamente 12543 = 3.37.113. Dado que el producto de 111 y 113 se realiza (en base 10) sin transporte de digitos, resulta

$$111/_{\langle 10\rangle}12543.$$

Por otra parte los productos 3.4181 y 37.339 requieren transporte de dígitos. Entonces los únicos $\langle 10\rangle$-divisores de 12543 son 1, 111, 113 y 12543.

8.3. Definición. a es $\langle p \rangle$-irreducible si se satisfacen:

I) $a \neq 1$;

II) $c /_{\langle p \rangle} a$ implica $c = 1$ o $c = a$.

8.4. Ejemplo. Los únicos divisores propios de 111 son 3 y 37. Dado que el producto de dichos números requiere transporte de dígitos, ocurre

111 es $\langle 10 \rangle$-irreducible.

Asimismo, puesto que 37 es primo, resulta

37 es $\langle 10 \rangle$-irreducible.

Las colecciones de $\langle p \rangle$-irreducibles y de $\langle p \rangle$-divisores de a se denotan $I^{\langle p \rangle}(Z^{\langle + \rangle})$ y $D^{\langle p \rangle}(a)$, respectivamente. La intersección de estas colecciones se denota $I^{\langle p \rangle}(a)$. Para $k = 0, 1, \ldots$ las intersecciones de $D^{\langle p \rangle}(a)$ e $I^{\langle p \rangle}(a)$ con $[p^k, p^{k+1})$ se denotan $D_k^{\langle p \rangle}(a)$ e $I_k^{\langle p \rangle}(a)$, respectivamente.

Se deduce trivialmente

8.5. Corolario. Si a es primo entonces a es $\langle p \rangle$-irreducible.

Más precisamente, dado que p/a implica $p /_{\langle p \rangle} a$, se tiene

8.6. Proposición. Son equivalentes:

i) a es primo;

ii) a es $\langle k \rangle$-irreducible ; $k = 2, 3, \ldots$;

iii) a es $\langle k \rangle$-irreducible ; k primo $< a^{1/2}$.

8.7. Nota. Una referencia excelente para tests de primalidad es [11]. Recientes avances se discuten en [12], [13], [14] y [15]. Por otra parte, si bien no se dispone actualmente de algoritmos eficientes para factorizar enteros arbitrarios (véanse [11] y [16]), no puede asegurarse aún, como justamente se remarca en [13], que tales algoritmos no existan.

De 7.1 y 8.1 se deduce

8.8. Corolario. Sea c/a. Son equivalentes:

i) $c /_{\langle p \rangle} a$;

ii) $a_{\langle p \rangle} = c_{\langle p \rangle} c^*_{\langle p \rangle}$.

8.9. **Nota.** Se verifican:

i) $/_{\langle p\rangle}$ es un orden parcial en $Z^{\langle +\rangle}\backslash\{0\}$;

ii) Las aplicaciones de 6.6 son isomorfismos entre los conjuntos parcialmente ordenados

$$(Z^{\langle p\rangle}[X]\backslash\{0\},\ /_{\langle +\rangle}) \quad \text{y} \quad (Z^{\langle +\rangle}\backslash\{0\},\ /_{\langle p\rangle}).$$

Se muestra a continuación que para determinar los $\langle p\rangle$-divisores y los $\langle p\rangle$-irreducibles, sólo hace falta la "mitad" de los enteros.

El polinomio

$$\mathrm{sim}(f) = X^{n}f(X^{-1})$$

se denomina simétrico de f. El número

$$\mathrm{sim}_{\langle p\rangle}(a) = \mathrm{sim}(a_{\langle p\rangle})(p)$$

se denomina p-simétrico de a.

Utilizando conocidas propiedades de sim(f), se deduce de 8.8 el resultado siguiente:

8.10. **Corolario.** Se verifican:

i) $c/_{\langle p\rangle}a$ sii $\mathrm{sim}_{\langle p\rangle}(c)/_{\langle p\rangle}\mathrm{sim}_{\langle p\rangle}(a)$;

ii) a es $\langle p\rangle$-irreducible sii $\mathrm{sim}_{\langle p\rangle}(a)$ es $\langle p\rangle$-irreducible.

Mostramos ahora como obtener divisores de $\mathrm{sim}_{\langle p\rangle}(a)$ a partir de los $\langle p\rangle$-divisores de a.

8.11. **Ejemplo.** Sea $p \geq 6$. Entonces (véase 8.2)

$$(113)_p /_{\langle p\rangle} (12543)_p.$$

Dado que $(12543)_p = (111)_p(113)_p$, por 8.10 se tiene $(311)_p /_{\langle p\rangle} (34521)_p$. Entonces

$$(34521)_p = (111)_p(311)_p.$$

En relación con la coprimalidad y separabilidad utilizaremos la terminología siguiente:

8.12. **Definición.** a y c son $\langle p\rangle$-coprimos si $b/_{\langle p\rangle}a$ y $b/_{\langle p\rangle}c$ implica $b = 1$.

8.13. **Definición.** a es $\langle p\rangle$-separable si $c^2/_{\langle p\rangle}a$ implica $c = 1$.

9. RELACION ENTRE $\langle + \rangle$ Y $\langle p \rangle$-DIVISIBILIDAD

Por 6.7 y 8.8, la relación existente entre $\langle + \rangle$ y $\langle p \rangle$-divisibilidad puede sintetizarse de la manera siguiente:

9.1. Teorema. $c \,/_{\langle p \rangle}{}^{a}_{\langle p \rangle}$ sii $c /_{\langle p \rangle} a$.

9.2. Corolario. Se verifican:

i) Las restricciones

$$\langle\langle p \rangle\rangle : D^{\langle + \rangle}(a_{\langle p \rangle}) \text{ -----} > D^{\langle p \rangle}(a),$$

$$\langle p \rangle : D^{\langle p \rangle}(a) \text{ -----} > D^{\langle + \rangle}(a_{\langle p \rangle}),$$

son biyectivas e inversas entre sí.

ii) I) $D^{\langle + \rangle}(a_{\langle p \rangle}) = \{b_{\langle p \rangle} : b /_{\langle p \rangle} a\}$;

II) $D^{\langle p \rangle}(a) = \{h(p) : h /_{\langle + \rangle}{}^{a}_{\langle p \rangle}\}$.

9.3. Ejemplo. Consideramos $a = 12543$ y $p = 10$. Ciertamente

$$a_{\langle p \rangle} = X^4 + 2X^3 + 5X^2 + 4X + 3.$$

Tenemos (véase 8.2)

$$D^{\langle p \rangle}(a) = \{1, 111, 113, 12543\}.$$

Entonces

$$D^{\langle + \rangle}(a_{\langle p \rangle}) = \{1, X^2 + X + 1, X^2 + X + 3, f\}.$$

Recíprocamente, conociendo

$$D^{\langle + \rangle}(a_{\langle p \rangle}) = \{1, X^2 + X + 1, X^2 + X + 3, f\},$$

evaluando en p resulta

$$D^{\langle p \rangle}(a) = \{1, 111, 113, 12543\}.$$

Es fácil ver entonces

9.4. Corolario. Para k = 0, 1, ... se verifican:

i) Las restricciones

$$\langle\langle p\rangle\rangle : D_k^{\langle+\rangle}(a_{\langle p\rangle}) \text{ -----> } D_k^{\langle p\rangle}(a),$$

$$\langle p\rangle : D_k^{\langle p\rangle}(a) \text{ -----> } D_k^{\langle+\rangle}(a_{\langle p\rangle}),$$

son biyectivas e inversas entre sí.

ii) I) $D_k^{\langle+\rangle}(a_{\langle p\rangle}) = \{b_{\langle p\rangle} : b/_{\langle p\rangle}a,\ p^k \leq b < p^{k+1}\}$;

II) $D_k^{\langle p\rangle}(a) = \{h(p) : h/_{\langle+\rangle}a_{\langle p\rangle},\ \text{grado}(h) = k\}$.

Podemos establecer ahora las siguientes condiciones necesarias y suficientes de $\langle+\rangle$-irreducibilidad:

9.5. Corolario. $a_{\langle p\rangle}$ es $\langle+\rangle$-irreducible sii a es $\langle p\rangle$-irreducible.

En particular ocurre

9.6. Corolario. Sea p > Sup{a,c}. Entonces

a coprimo con c sii ap + c es $\langle p\rangle$-irreducible.

Por 6.6 se tienen las "descripciones paramétricas" siguientes:

9.7. Corolario. Se verifican:

i) $I(Z^{\langle+\rangle}[X]) = \{b_{\langle p\rangle} : b \in I^{\langle p\rangle}(Z^{\langle+\rangle})\}$;

ii) $I^{\langle p\rangle}(Z^{\langle+\rangle}) = \{h(p) : h \in I(Z^{\langle+\rangle}[X])\}$.

9.8. Corolario. Se verifican:

i) Las restricciones

$$\langle\langle p\rangle\rangle : I^{\langle+\rangle}(a_{\langle p\rangle}) \text{ -----> } I^{\langle p\rangle}(a),$$

$$\langle p\rangle : I^{\langle p\rangle}(a) \text{ -----> } I^{\langle+\rangle}(a_{\langle p\rangle}),$$

son biyectivas e inversas entre sí.

ii) I) $I^{\langle+\rangle}(a_{\langle p\rangle}) = \{b_{\langle p\rangle} : b \in I^{\langle p\rangle}(a)\}$;

II) $I^{\langle p\rangle}(a) = \{h(p) : h \in I^{\langle+\rangle}(a_{\langle p\rangle})\}$.

9.9. Nota. Luego, las restricciones de 9.2 también preservan factorizaciones (no necesariamente únicas por 3.4).

9.10. Ejemplo. Sean $a = 12543$ y $p = 10$. Luego

$$a_{\langle p\rangle} = X^4 + 2X^3 + 5X^2 + 4X + 3.$$

Tenemos entonces (véanse 8.2, 8.4 y 9.3)

$$I^{\langle p\rangle}(a) = \{111, 113\}.$$

En consecuencia

$$I^{\langle+\rangle}(a_{\langle p\rangle}) = \{X^2 + X + 1, X^2 + X + 3\}.$$

Recíprocamente, conociendo

$$I^{\langle+\rangle}(a_{\langle p\rangle}) = \{X^2 + X + 1, X^2 + X + 3\},$$

evaluando en p se obtiene

$$I^{\langle p\rangle}(a) = \{111, 113\}.$$

Entonces, de 9.4 y 9.8 se deduce

9.11. Corolario. Para $k = 0, 1, \ldots$ se verifican:

i) Las restricciones

$$\langle\langle p\rangle\rangle : I_k^{\langle+\rangle}(a_{\langle p\rangle}) \text{ -----> } I_k^{\langle p\rangle}(a),$$

$$\langle p\rangle : I_k^{\langle p\rangle}(a) \text{ -----> } I_k^{\langle+\rangle}(a_{\langle p\rangle}),$$

son biyectivas e inversas entre sí.

ii) I) $I_k^{\langle+\rangle}(a_{\langle p\rangle}) = \{b_{\langle p\rangle} : b \in I_k^{\langle p\rangle}(a)\}$;

II) $I_k^{\langle p\rangle}(a) = \{h(p) : h \in I_k^{\langle+\rangle}(a_{\langle p\rangle})\}$.

Las intersecciones de las colecciones $D^{\langle+\rangle}(a_{\langle p\rangle})$, $D^{\langle+\rangle}(c_{\langle p\rangle})$ y $D^{\langle p\rangle}(a)$, $D^{\langle p\rangle}(c)$, se denotan $D^{\langle+\rangle}(a_{\langle p\rangle}, c_{\langle p\rangle})$ y $D^{\langle p\rangle}(a,c)$, respectivamente.

De 9.2 se deduce

9.12. **Corolario.** Las restricciones

$$\langle\langle p\rangle\rangle : D^{\langle+\rangle}(a_{\langle p\rangle}, c_{\langle p\rangle}) \text{ -----} > D^{\langle p\rangle}(a,c),$$

$$\langle p\rangle : D^{\langle p\rangle}(a,c) \text{ -----} > D^{\langle+\rangle}(a_{\langle p\rangle}, c_{\langle p\rangle}),$$

son biyectivas e inversas entre si.

En consecuencia

9.13. **Corolario.** $a_{\langle p\rangle}$ y $c_{\langle p\rangle}$ son $\langle+\rangle$-coprimos sii a y c son $\langle p\rangle$-coprimos.

9.14. **Corolario.** $a_{\langle p\rangle}$ es $\langle+\rangle$-separable sii a es $\langle p\rangle$-separable.

10. CARACTERIZACION DE LOS $\langle P\rangle$-DIVISORES

Por 7.1, 8.8 y 9.1, con $a_{\langle p\rangle}$ y $c_{\langle p\rangle}c^*_{\langle p\rangle}$ en lugar de f y g, respectivamente, los $\langle p\rangle$-divisores de a se caracterizan, entre los divisores de a, mediante condiciones aritméticas sencillas. En primer lugar, de 4.5 se deduce el hecho siguiente:

10.1. **Teorema.** Sea c/a. Son equivalentes:

i) $c/_{\langle p\rangle}a$;

ii) $c_k(p)c_0^*(p) + c_{k-1}(p)c_1^*(p) + \ldots + c_0(p)c_k^*(p) < p \ ; \ k = 0, \ldots, n_p(c) + n_p(c^*)$;

10.2. **Nota.** c/a implica $n_p(a) - 1 \leq n_p(c) + n_p(c^*) \leq n_p(a)$.

El entero

$$|a|_p = a_{\langle p\rangle}(1) = a_{n_p}(p) + \ldots + a_1(p) + a_0(p)$$

se denomina p-altura de a.

Razonando inductivamente se prueba (observación de E. R. Gentile)

10.3. **Proposición.** $|a + c|_p \leq |a|_p + |c|_p$.

La desigualdad triangular 10.3 sigue vigente para enteros arbitrarios cuando se define

$$|0|_p = 0 \quad , \quad |-a|_p = |a|_p .$$

Luego, $d_p : ZxZ \dashrightarrow R : d_p(x,y) = |y - x|_p$ es una métrica en Z. Por otra parte y de acuerdo con 8.2, la p-altura no es un valor absoluto. Este hecho se debe a que los $\langle p \rangle$-divisores admiten, en virtud de 4.8 y 6.4, la siguiente caracterización:

10.5. **Teorema.** Sea c/a. Son equivalentes:

i) $c/_{\langle p \rangle}a$;

ii) $|a|_p = |c|_p |c^*|_p$.

10.6. **Ejemplo.** Obviamente (véase 8.2)

$$|12543|_{10} = 15 \ , \ |111|_{10} = 3 \ , \ |113|_{10} = 5.$$

Puesto que

$$|12543|_{10} = |111|_{10}|113|_{10}$$

ocurre

$$111/_{\langle 10 \rangle}12543.$$

De 3.10 y 10.5 resulta

10.7. **Corolario.** Sea a > 1. Entonces a es $\langle p \rangle$-irreducible o bien a tiene un $\langle p \rangle$-divisor propio b (esto es, distinto de 1 y de b) verificando cualquiera de las afirmaciones siguientes:

I) $b \leq a^{1/2}$;

II) $r_p(b) \leq r_p(a)^{1/2}$;

III) $|b|_p \leq |a|_p^{1/2}$.

Además, si b satisface alguna de las condiciones mencionadas, digamos *), y b es el mínimo entre los $\langle p \rangle$-divisores propios de a que satisfacen *), entonces b es $\langle p \rangle$-irreducible.

Consideramos ahora el entero

$$E_p(a) = [a/p] + [a/p^2] + \ldots + [a/p^{np}].$$

Es un hecho bien conocido (Legendre; véase [17])

10.8. **Proposición.** Si p es primo entonces $E_p(a)$ es el exponente de p en a!.

Por otra parte, por 6.3, evaluando en 1 obtenemos

10.9. **Corolario.** $|a|_p = a - (p - 1)\, E_p(a)$.

Entonces, reformulamos 10.5 como sigue:

10.10. **Teorema.** Sea c/a. Son equivalentes:

i) $c/_{\langle p\rangle} a$;

ii) $E_p(a) = c^{*}E_p(c) + cE_p(c^{*}) - (p - 1)\, E_p(c)E_p(c^{*})$.

10.11. **Ejemplo.** Se tiene $([a/p^{k+1}] = [[a/p^{k}]/p];\ k = 0, 1, \ldots)$

$$E_{10}(12543) = 1254 + 125 + 12 + 1 = 1392,$$

$$E_{10}(111) = 11 + 1 = 12\ ,\ E_{10}(113) = 11 + 1 = 12.$$

Dado que

$$1392 = 113.12 + 111.12 - 9.12.12$$

resulta

$$111/_{\langle 10\rangle} 12543.$$

Si p es primo y x es racional no nulo, la norma p-ádica de x está definida (véase [18])

$$Np(x) = p^{-ep(x)},$$

donde $e_p(x)$ es el exponente de p en x.

De 10.8, 10.9 y 10.10 resulta la siguiente caracterización de los $\langle p\rangle$-divisores:

10.12. **Teorema.** Suponemos p primo. Sea c/a. Son equivalentes:

i) $c/_{\langle p\rangle} a$;

ii) $N_p(a!/(c!^{c^{*}}c^{*}!^{|c|_p})) = 1$.

Además, de 4.10 deducimos

10.13. **Teorema.** Sea c/a. Son equivalentes:

i) $c/_{\langle p\rangle} a$;

ii) $a'_{\langle p\rangle}(p) = c^{*}c'_{\langle p\rangle}(p) + cc^{*\prime}_{\langle p\rangle}(p)$.

10.14. **Nota.** De 6.3, derivando y evaluando en p, obtenemos

$$(a_{\langle p\rangle})'(p) = [a/p] + [a/p]p^2 + \dots + [a/p^{np}]p^{np-1}.$$

El carácter aditivo de 10.13 puede ponerse de manifiesto considerando la p-altura logarítmica de a, definida (ln = logaritmo natural)

$$|\!|a|\!|_p = a'_{\langle p\rangle}(p)/a = (\ln a_{\langle p\rangle})'(p).$$

Entonces, 10.13 presenta el aspecto siguiente:

10.15. **Teorema.** Sea c/a. Son equivalentes:

i) $c/_{\langle p\rangle}a$;

ii) $|\!|a|\!|_p = |\!|c|\!|_p + |\!|c^*|\!|_p$.

A continuación generalizamos 10.1, 10.5 y 10.15 (con a= bc...l).

10.16. **Corolario.** Sean b, ... , l enteros positivos. Son equivalentes:

i) $(bc\dots l)_{\langle p\rangle} = b_{\langle p\rangle}c_{\langle p\rangle}\dots l_{\langle p\rangle}$;

ii) $b_k(p)c_0(p)\dots l_0(p) + \dots + b_0(p)c_0(p)\dots l_k(p) < p$; $k = 0, \dots, n_p(b) + \dots + n_p(l)$;

iii) $|bc\dots l|_p = |b|_p|c|_p\dots|l|_p$;

iv) $|\!|bc\dots l|\!|_p = |\!|b|\!|_p + |\!|c|\!|_p + \dots + |\!|l|\!|_p$.

El número de $\langle p\rangle$-divisores de a que no son potencias de p y cuyo producto es a puede acotarse entonces de la manera siguiente:

10.17. **Corolario.** Sean k entero ≥ 1 y $b_1, b_2, \dots b_k$ $\langle p\rangle$-divisores de a tales que

I) $|b_i|_p \geq 2$; $i = 1, 2, \dots, k$;

II) $a = b_1b_2\dots b_k$.

Entonces

$$k \leq \log_2(|a|_p).$$

Por otra parte, de 6.1 se deduce

10.18. **Corolario.** $|a|_p \leq (p - 1)(1 + \log_p a)$.

Utilizamos seguidamente la bien conocida notación O. Dado que

$$\log_p a = O(\ln a),$$

se tiene (fijando p)

$$|a|_p = O(\ln a).$$

En resumidas cuentas, es un hecho

10.19. **Proposición.** Sean k y $b_1, b_2, \ldots, b_k$ como en 10.17. Entonces

$$k = O(\ln\ln a).$$

10.20. **Nota.** Asumiendo únicamente

I) $b_i \geq 2$; $i = 1, 2, \ldots, k$;

II) $a = b_1 b_2 \ldots b_k$,

solamente puede asegurarse

$$k = O(\ln a).$$

11. CONDICIONES SUFICIENTES PARA <P>-COPRIMALIDAD Y <P>-IRREDUCIBILIDAD

En relación con la coprimalidad tenemos

11.1. **Proposición.** Si p no es divisor de a entonces

$$|a|_p \text{ coprimo con } |c|_p \text{ implica a } \langle p\rangle\text{-coprimo con c.}$$

Prueba. Suponemos a > 1 no divisible por p y $|a|_p$ coprimo con $|c|_p$. Sea b > 1 tal que $b/_{\langle p\rangle}a$ y $b/_{\langle p\rangle}c$. Esto implica

$$|a|_p = |b|_p |b^*(a)|_p \ , \ |c|_p = |b|_p |b^*(c)|_p.$$

En consecuencia

$$|a|_p |b^*(c)|_p = |c|_p |b^*(a)|_p.$$

Entonces, resulta

$$|a|_p / |b^*(a)|_p.$$

Luego

$$|b|_p = 1.$$

Dado que p no es divisor de b, la conclusión sigue de la contradicción b = 1.#

En conexión con la <p>-irreducibilidad ocurre

11.2. **Proposición.** Si p no es divisor de a entonces

$$|a|_p \text{ primo implica a } \langle p\rangle\text{-irreducible.}$$

Prueba. Suponemos a no divisible por p y $|a|_p$ primo. Sea $c/_{\langle p\rangle}a$. Por 10.3 tenemos

$$|a|_p = |c|_p |c^*|_p.$$

Luego

$$|a|_p \text{ primo implica } |c|_p = 1 \text{ o } |c^*|_p = 1.$$

Dado que p no es divisor de a, resulta

$$c = 1 \text{ o } c^* = 1.\#$$

12. NUMEROS DE MERSENNE

Son los enteros (bien conocidos por otra parte) de la forma

$$M_a = 2^a - 1.$$

En primer lugar se tiene

12.1. **Proposición.** Se verifican:

i) I) $M_a = 2^{a-1} + 2^{a-2} + \ldots + 2 + 1$;

II) $|M_a|_2 = a$.

ii) $M_{ac} = M_a((2^a)^{c-1} + (2^a)^{c-2} + \ldots + 2^a + 1)$.

Entonces, se deduce (Cataldi-Fermat; véanse [2] y [10])

12.2. **Corolario.** Si M_a es primo entonces a es primo.

12.3. **Nota.** El recíproco de 12.2 es falso. Por ejemplo, $M_{11} = 2047 = 23.89$.

Modificaremos adecuadamente 12.2 de manera que la implicación se torne equivalencia. De 12.1 deducimos

12.4. **Corolario.** Si M_a es $\langle 2\rangle$-irreducible entonces a es primo.

Por otra parte, de 11.2 y 12.1, resulta

12.4. **Corolario.** Si a es primo entonces M_a es $\langle 2\rangle$-irreducible.

Por 12.3 y 12.4 caracterizamos los $\langle 2\rangle$-irreducibles de Mersenne como sigue (véase 8.6):

12.5. **Teorema.** M_a es $\langle 2\rangle$-irreducible sii a es primo.

12.6. **Ejemplo.** "Probamos" aquí que 11 es primo (véanse 10.5 y 12.3).

$$M_{11} = (11111111111)_2 \ , \ |M_{11}|_2 = 11,$$

$$23 = (10111)_2 \ , \ |23|_2 = 4,$$

$$89 = (1010101)_2 \ , \ |89|_2 = 4,$$

M_{11} es $\langle 2\rangle$-irreducible;

11 es primo.

Claramente ocurre

$$(M_a)_{\langle 2\rangle} = X^{a-1} + X^{a-2} + \ldots + X + 1.$$

Entonces, por 9.5 se tiene

12.7. **Corolario.** $(M_a)_{\langle 2\rangle}$ es $\langle +\rangle$-irreducible sii a es primo.

12.8. **Nota.** Es bien conocido el hecho siguiente (polinomios ciclotómicos):

$(M_a)_{\langle 2\rangle}$ es irreducible sii a es primo.

Obviamente, de 12.5 se deduce

12.9. **Corolario.** M_{M_a} es $\langle 2\rangle$-irreducible sii M_a es primo.

12.10. **Nota.** Son hechos bien conocidos (véase [10]):

i) **Teorema** (Lucas-Lehmer). Sea a primo impar. Se define

$$S_1 = 4 \ , \ S_{k+1} = S_k^2 - 2 \ ; \ k = 1, 2, \ldots \ ,.$$

Entonces

$$M_a \text{ es primo sii } M_a / S_{a-1}.$$

ii) La conjetura de Catalan

$$M_a \text{ primo implica } M_{M_a} \text{ primo,}$$

fue refutada como sigue (Wheeler):

$$M_{13} \text{ primo y } M_{M_{13}} \text{ compuesto.}$$

13. CARACTERIZACION ARITMETICA DE LOS ⟨+⟩-DIVISORES

Reuniendo y reformulando 9.2, 9.4, 9.5, 9.8 y 9.11 resulta

13.1. Teorema. Sea $p > r(f)$. Se verifican:

i) I) Las restricciones

$$\langle\langle p\rangle\rangle : D^{\langle+\rangle}(f) \text{ -----> } D^{\langle p\rangle}(f(p)),$$

$$\langle p\rangle : D^{\langle p\rangle}(f(p)) \text{ -----> } D^{\langle+\rangle}(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $D^{\langle+\rangle}(f) = \{b_{\langle p\rangle} : b \in D^{\langle p\rangle}(f(p))\}$.

ii) Sea $k = 0, 1, \ldots, n$. Entonces

I) Las restricciones

$$\langle\langle p\rangle\rangle : D_k^{\langle+\rangle}(f) \text{ -----> } D_k^{\langle p\rangle}(f(p)),$$

$$\langle p\rangle : D_k^{\langle p\rangle}(f(p)) \text{ -----> } D_k^{\langle+\rangle}(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $D_k^{\langle+\rangle}(f) = \{b_{\langle p\rangle} : b \in D_k^{\langle p\rangle}(f(p))\}$.

iii) f es ⟨+⟩-irreducible sii f(p) es ⟨p⟩-irreducible.

iv) I) Las restricciones

$$\langle\langle p\rangle\rangle : I^{\langle+\rangle}(f) \text{ -----> } I^{\langle p\rangle}(f(p)),$$

$$\langle p\rangle : I^{\langle p\rangle}(f(p)) \text{ -----> } I^{\langle+\rangle}(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $I^{\langle+\rangle}(f) = \{b_{\langle p\rangle} : b \in I^{\langle p\rangle}(f(p))\}$.

v) Sea k = 0, 1, ... , n. Entonces

I) Las restricciones

$$\langle\langle p\rangle\rangle : I_k^{(+)}(f) \text{ -----} > I_k^{\langle p\rangle}(f(p)),$$

$$\langle p\rangle : I_k^{\langle p\rangle}(f(p)) \text{ -----} > I_k^{(+)}(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $I_k^{(+)}(f) = \{b_{\langle p\rangle} : b \in I_k^{\langle p\rangle}(f(p))\}$.

13.2. **Nota.** El teorema previo sigue vigente (caracterización residual de los $\langle+\rangle$-divisores; vease [19]) con las reinterpretaciones siguientes (como es habitual, Z_p denota el anillo de clases de enteros módulo p):

i) f(p) es el polinomio de $Z_p[Y]$ cuyo coeficiente de orden k es la clase módulo p del coeficiente de orden k de f;

ii) El p-polinomio de $F \in Z_p[Y]$, es el polinomio $F_{\langle p\rangle} \in Z[X]$ cuyo coeficiente de orden k es el menor representante no negativo en la clase del coeficiente de orden k de F;

iii) Si $F, G \in Z_p[Y]$ entonces

I) $G/_{\langle p\rangle}F$ equivale a G/F y $F_{\langle p\rangle} = G_{\langle p\rangle}G^{*}_{\langle p\rangle}$;

II) F se dice $\langle p\rangle$-irreducible si $F \neq 1$ y además $G/_{\langle p\rangle}F$ implica $G = 1$ o $G = F$.

Asimismo, el enunciado que se obtiene de 4.6 al reemplazar $f = g + (X - p)h$ por $f = g + ph$ es un hecho que permite probar

$$G/_{\langle p\rangle}F \text{ sii } G_{\langle p\rangle}(p)/_{\langle p\rangle}F_{\langle p\rangle}(p).$$

Por otra parte, la factorización de polinomios con coeficientes módulo p mediante el algoritmo de Berlekamp (y su aplicación a la factorización en Z[X]) puede verse en [11].

14. CONDICIONES SUFICIENTES PARA $\langle+\rangle$-COPRIMALIDAD Y $\langle+\rangle$-SEPARABILIDAD

Reformulando 11.1 se obtiene

14.1. Corolario. Si $f(0) \neq 0$ entonces

$f(1)$ coprimo con $g(1)$ implica f $\langle+\rangle$-coprimo con g.

Entonces, resulta

14.2. Corolario. Si $f(0) \neq 0$ entonces

$f(1)$ coprimo con $f'(1)$ implica f $\langle+\rangle$-separable.

El próximo resultado complementa 1.14. Una de sus afirmaciones es consecuencia directa de 14.2, la restante se establece derivando y evaluando en q ambos miembros de $f = gg^*$.

14.3. Corolario. Suponemos $q \geq 1$. Sea $f'(q)$ primo. Entonces:

i) f es $\langle+\rangle$-separable;

ii) $g/_{\langle+\rangle}f$ implica $g(q)$ coprimo con $g^*(q)$.

15. CONDICIONES SUFICIENTES PARA $\langle+\rangle$-IRREDUCIBILIDAD Y $\langle+\rangle$-IRREDUCIBILIDAD TOTAL

En primer lugar reformulamos 11.2.

15.1. Proposición. Si $f(0) \neq 0$ entonces

$f(1)$ primo implica f totalmente $\langle+\rangle$-irreducible.

Ahora extendemos 15.1.

15.2. Proposición. Sean a primo y $p > c$. Entonces

$f(p) = ac$ implica f_{prim} $\langle+\rangle$-irreducible.

Prueba. Si $c = 1$ la conclusión sigue de 15.1. Suponemos entonces $c > 1$. Sea $g/_{\langle+\rangle}f$. Podemos asumir

$$g \text{ } \langle+\rangle\text{-irreducible} \text{ , } g(p) = ba \text{ ; } b/c.$$

Esto implica

$$g^*(p) = b^* = c/b.$$

Dado que $b^* < p$, resulta $g^* = b^* = c(f)$.#

Con $c = d(f)$ obtenemos

15.3. Corolario. Sea f primitivo. Si $p > d(f)$ entonces

$f(p)/d(f)$ primo implica f $\langle+\rangle$-irreducible.

De manera semejante, utilizando 1.14 y 14.3 probamos

15.4. **Proposición.** Suponemos f primitivo y separable. Sean k entero ≥ 1, $p > c$ y a primo tales que

$$f(p) = a^k c.$$

Suponemos además que alguna de las condiciones siguientes se satisface:

I) f(0) separable y res $(f, f')/p$;

II) $f'(p)$ primo.

Entonces

f es $\langle + \rangle$-irreducible.

En consecuencia

15.5. **Corolario.** Suponemos f primitivo y separable. Sean k entero ≥ 1 y a primo tales que

$$f(p)/d(f) = a^k.$$

Suponemos además que alguna de las condiciones siguientes se satisface:

I) f(0) separable y res $(f, f')/p$;

II) $f'(p)$ primo.

Entonces

f es $\langle + \rangle$-irreducible.

16. CARACTERIZACION ARITMETICA DE LOS DIVISORES

Suprimimos ahora la restricción f y g no negativos. Eligiendo q de modo que f_q sea cuasi-estable, teniendo en cuenta 2.4, 2.5 y 2.6, aplicando 13.1 a f_q y retornando a los divisores de f mediante 1.20, resulta la siguiente "parte derecha" de la caracterización aritmética de los divisores de f (la parte restante se establece de manera semejante con $(-1)^n f(-X)$ en lugar de f):

16.1. **Teorema.** Sean q y p tales que

I) Las raíces de f se encuentran en el semiplano $Re(z) \leq q$;

II) $p > r(f_q)$ (esto es, $p > Sup_{k=0,1,\ldots} f^{(k)}(q)/k!$).

Se verifican:

i) I) Las restricciones

$$\langle\langle p+q\rangle\rangle : D(f) \text{ -----> } D^{\langle p\rangle}(f(p+q)),$$

$$\langle p\rangle : D^{\langle p\rangle}(f(p+q)) \text{ -----> } D(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $D(f) = \{b_{\langle p\rangle}(X-q) : b \in D^{\langle p\rangle}(f(p+q))\}$.

ii) Sea $k = 0, 1, \ldots, n$. Entonces

I) Las restricciones

$$\langle\langle p+q\rangle\rangle : D_k(f) \text{ -----> } D_k^{\langle p\rangle}(f(p+q)),$$

$$\langle p\rangle : D_k^{\langle p\rangle}(f(p+q)) \text{ -----> } D_k(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $D_k(f) = \{b_{\langle p\rangle}(X-q) : b \in D_k^{\langle p\rangle}(f(p+q))\}$.

iii) f es irreducible sii f(p+q) es $\langle p\rangle$-irreducible.

iv) I) Las restricciones

$$\langle\langle p+q\rangle\rangle : I(f) \text{ -----> } I^{\langle p\rangle}(f(p+q)),$$

$$\langle p\rangle : I^{\langle p\rangle}(f(p+q)) \text{ -----> } I(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $I(f) = \{b_{\langle p\rangle}(X-q) : b \in I^{\langle p\rangle}(f(p+q))\}$.

v) Sea $k = 0, 1, \ldots, n$. Entonces

I) Las restricciones

$$\langle\langle p+q\rangle\rangle : I_k(f) \text{ -----> } I_k^{\langle p\rangle}(f(p+q)),$$

$$\langle p\rangle : I_k^{\langle p\rangle}(f(p+q)) \text{ -----> } I_k(f),$$

están bien definidas y son biyectivas e inversas entre sí;

II) $I_k(f) = \{b_{\langle p\rangle}(X-q) : b \in I_k^{\langle p\rangle}(f(p+q))\}$.

16.2. **Ejemplos.** Ilustramos 16.1 con el polinomio

$$f = X^2 - 3X + 2.$$

Por 1.24 podemos elegir

$$q = 4.$$

Dado que

$$f(X+q) = X^2 + 5X + 6,$$

elegimos

$$p = 7.$$

Sea

$$a = f(p+q) = 90.$$

Entonces

$$D^{\langle + \rangle}(a) = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}.$$

$$D^{\langle p \rangle}(a) = \{1, 9, 10, 90\},$$

$$D^{\langle + \rangle}(a_{\langle p \rangle}) = \{1, X + 2, X + 3, f_q\},$$

$$D(f) = \{1, X - 2, X - 1, f\},$$

$$f = (X - 2)(X - 1).$$

Consideramos también el polinomio

$$f = X^2 + X + 1.$$

Por 1.24 podemos elegir

$$q = 2.$$

Dado que

$$f(X+q) = X^2 + 5X + 7,$$

elegimos

$$p = 8.$$

Sea

$$a = f(p+q) = 111.$$

Luego

$$D^{\langle + \rangle}(a) = \{1, 3, 37, 111\},$$

$$D^{\langle p \rangle}(a) = \{1, 111\}.$$

Entonces

$$a \text{ es } \langle p \rangle\text{-irreducible.}$$

En consecuencia

$$f \text{ es irreducible.}$$

Por 1.21 y 1.24 las hipótesis de 16.1 se satisfacen cuando $q \geq q(f)$ y $p \geq p(f)$, donde $q(f)$ y $p(f)$ son los enteros definidos como sigue:

$$q(f) = 1 + r_{-1}(f),$$

$$p(f) = 1 + (2 + r_{-1}(f))^{n} r_{-1}(f).$$

Análogamente, en el caso f no negativo, por 1.29 podemos definir

$$q(f) = \mathrm{Inf}\{b \in Z : b \geq (1 + r(f))^{1/2}\};$$

$$p(f) = \mathrm{Inf}\{b \in Z : b > (1 + (1 + r(f))^{1/2})^{n} r(f)\}.$$

Se tiene entonces el siguiente criterio de irreducibilidad:

16.3. **Corolario.** f es irreducible sii $f(p(f)+q(f))$ es $\langle p(f)\rangle$-irreducible.

16.4. **Nota.** Por lo dicho en 13.2, la caracterización residual de los divisores de f se establece con el mismo enunciado de 16.1, salvo el reemplazo de $f(p+q)$ por el valor de f_q en p (también existe un análogo de 16.3). Estas caracterizaciones se mantienen, con los cambios notacionales correspondientes, cuando se reemplaza Z por cualquier dominio real cuyos elementos positivos estén bien ordenados. En particular, las cuestiones relativas a polinomios en varias indeterminadas con coeficientes enteros se reducen al caso de polinomios en una indeterminada (véase [20]). Con mayor generalidad, esto también ocurre para polinomios en varias indeterminadas con coeficientes en dominios arbitrarios (véase [21]). Como corolario resultan condiciones necesarias y suficientes de irreducibilidad absoluta para polinomios con coeficientes en campos arbitrarios. Un tratamiento unificado puede verse en [22].

17. CARACTERIZACION ARITMETICA DE COPRIMALIDAD Y SEPARABILIDAD

El máximo común divisor de f y g en Z[X] se denota d(f,g). Por 9.12 y 16.1 i) ocurre

17.1. **Corolario.** Sean q y p tales que

I) Las raíces de fg se encuentran en el semiplano $\mathrm{Re}(z) \leq q$;

II) $p > \mathrm{Sup}(r(f_q), r(g_q))$.

Sea d el máximo común divisor de $a = f(p+q)$ y $c = g(p+q)$. El mayor divisor de d que es $\langle p\rangle$-divisor común de $f(p+q)$ y $g(p+q)$ se denota b. Entonces

$$d(f,g) = b_{\langle p\rangle}(X-q).$$

17.2. **Ejemplo.** Sean $f = X^2 - 3X + 2$ y $g = X^2 - 2X + 1$. Por 1.24 podemos elegir

$$q = 4.$$

Dado que ocurre

$$f(X+q) = X^2 + 5X + 6 \quad , \quad g(X+q) = X^2 + 6X + 9,$$

elegimos

$$p = 10.$$

Sean

$$a = f(p+q) = 156 \quad , \quad c = g(p+q) = 169.$$

Calculando el máximo común divisor de a y c se obtiene d = 13. Ciertamente

$$13/_{\langle 10\rangle}156 \ , \ 13/_{\langle 10\rangle}169.$$

Puesto que

$$13_{\langle 10\rangle} = X + 3,$$

resulta

$$d(f,g) = X - 1.$$

Entonces, podemos establecer los resultados siguientes:

17.3. **Teorema.** Sean q y p como en 17.1. Entonces

f y g son coprimos sii f(p+q) y g(p+q) son $\langle p\rangle$-coprimos.

17.4. **Teorema.** Sean q y p tales que

I) Las raíces de f se encuentran en el semiplano $Re(z) \leq q$;

II) $p > Sup(r(f_q), r(f_q'))$.

Entonces

f es separable sii f(p+q) es $\langle p\rangle$-separable.

17.5. **Ejemplo.** Consideramos el polinomio

$$f = X^2 - 3X + 2$$

Con q = 4 y p = 7 se tiene (véase 16.3)

$$D^{\langle p\rangle}(f(p+q)) = \{1, 9, 10, 90\}.$$

Luego

f(p+q) es $\langle p\rangle$-separable.

Entonces

f es separable.

18. CONDICIONES SUFICIENTES PARA COPRIMALIDAD Y SEPARABILIDAD

Asumimos momentáneamente

I) Las raíces de fg se encuentran en el semiplano $Re(z) \leq q$;

II) $p > Sup\{r(f_q), r(g_q)\}$.

De 17.1 deducimos

18.1. Corolario. Suponemos f primitivo. Sea d el máximo común divisor de f(p+q) y g(p+q). Entonces

$$d < p \text{ implica } f \text{ coprimo con } g.$$

18.2. Corolario. Suponemos f primitivo. Sea d el máximo común divisor de f(p+q) y f'(p+q). Entonces

$$d < p \text{ implica } f \text{ separable.}$$

Por otra parte, de 14.1 resulta

18.3. Corolario. Si $f(q) \neq 0$ entonces

f(q+1) coprimo con g(q+1) implica f coprimo con g.

Considerando g = 1 se tiene

18.4. Corolario. Sea $f(q) \neq 0$. Entonces

f(q+1) coprimo con f'(q+1) implica f separable.

Por 14.3 resulta

18.5. Corolario. Suponemos $f(q) \neq 0$. Sea f'(q+1) primo. Entonces:

i) f es separable;

ii) $g/_{\langle + \rangle} f$ implica g(q+1) coprimo con $g^*(q+1)$.

Ya sin restricciones sobre q y p mejoramos 18.3 y consecuentemente 18.4 y 18.5.

18.6. Proposición. Sea q tal que

I) Las raíces de f se encuentran en el semiplano $Re(z) < q + 1/2$;

II) $f(q) \neq 0$.

Entonces

f(q+1) coprimo con g(q+1) implica f coprimo con g.

Prueba. Suponemos f(q+1) coprimo con g(q+1). Sea h ∈ Z[X], h con coeficiente principal positivo, divisor común de h y g. Luego

$$h(q+1) = 1.$$

Además, h tiene sus raíces en el semiplano

$$Re(z) < q + 1/2.$$

Suponemos ahora h de grado positivo. Por 2.7. resulta

$$|h(q)| < h(q+1).$$

En consecuencia

$$h(q) = 0.$$

Resulta entonces la contradicción

$$f(q) = 0.$$

Luego

$$h = h(q+1) = 1.\#$$

18.7. Corolario. Sea q tal que

I) Las raíces de f se encuentran en el semiplano $Re(z) < q + 1/2$;

II) $f(q) \neq 0$.

Entonces

f(q+1) coprimo con f'(q+1) implica f separable.

18.8. Corolario. Sea q tal que

I) Las raíces de f se encuentran en el semiplano $Re(z) < q + 1/2$;

II) $f(q) \neq 0$;

III) f'(q+1) primo.

Entonces

i) f es separable;

ii) g/f implica g(q+1) coprimo con g*(q+1).

19. CONDICIONES SUFICIENTES PARA IRREDUCIBILIDAD E IRREDUCIBILIDAD TOTAL

Seguidamente extenderemos a polinomios arbitrarios las condiciones suficientes de ⟨+⟩-irreducibilidad y ⟨+⟩-irreducibilidad total obtenidas oportunamente.

De 2.5, 2.6 y 15.1 deducimos

19.1 **Corolario.** Sea q tal que

I) Las raíces de f se encuentran en el semiplano $Re(z) \leq q$;

II) $f(q) \neq 0$.

Entonces

$f(q+1)$ primo implica f totalmente irreducible.

De aquí resulta (Brillhart, 1983; véase [23], citado en [24])

19.2. **Corolario.** Si las raíces de f se encuentran en el disco $|\ | < q$ entonces

$f(q+1)$ primo implica f irreducible.

A su vez, 19.1 se deduce del inmejorable resultado siguiente (Gmelin-Pólya, 1918-1919; véase [7]):

19.3. **Teorema.** Sea q tal que

I) Las raíces de f se encuentran en el semiplano $Re(z) < q + 1/2$;

II) $f(q) \neq 0$.

Entonces

$f(q+1)$ primo implica f totalmente irreducible.

Prueba. Suponemos $f(q+1)$ primo. Sea g/f. Ciertamente

$$g(q+1) = 1 \quad o \quad g^{\#}(q+1) = 1.$$

Por 18.7 resulta

$$g = 1 \quad o \quad g^{\#} = 1.$$

Esto prueba f irreducible. Asimismo, por 2.7 tenemos

$$|f(q)| < f(q+1).$$

Dado que $f(q+1)$ es primo la desigualdad previa implica

$$d(f) = 1.\#$$

19.4. **Nota.** Si en 19.3 la constante 1/2 (en I)) se reemplaza por cualquier real w en el intervalo $1/2 < w < 1$, la conclusión es falsa. Por ejemplo, el polinomio

$$g = (X + p - q - 1)(p(X - q - 1) + 1)^{m-1},$$

es totalmente primitivo, tiene sus raíces en el semiplano $Re(z) < q + w$, no se anula en q y asume un valor arbitrario $p < 1/(1 - w)$ en $q + 1$.

Por otra parte, por 15.2 podemos extender 19.1 como sigue:

19.5. Corolario. Sean q y p tales que

I) Las raíces de f se encuentran en el semiplano $\mathrm{Re}(z) \leq q$;

II) a primo y $p > c$.

Entonces

$$f(p+q) = ac \text{ implica } f_{prim} \text{ irreducible.}$$

En consecuencia

19.6. Corolario. Suponemos f primitivo. Sean q y p tales

I) Las raíces de f se encuentran en el semiplano $\mathrm{Re}(z) \leq q$;

II) $p > d(f)$.

Entonces

$$f(p+q)/d(f) \text{ primo implica } f \text{ irreducible.}$$

19.7. Corolario. Si $f/d(f)$ representa infinitos primos entonces f es irreducible.

19.8. Nota. El recíproco de 19.7 es actualmente una conjetura (de V. Bouniakowsky; véase [2]).

Entonces, resulta

19.9. Corolario. Si f representa infinitos primos entonces f es totalmente irreducible.

19.10. Nota. El recíproco de 19.9 ha sido probado parcialmente por Dirichlet (en el caso $n = 1$) en su Teorema sobre los primos en progresión aritmética (véase [25]) y es consecuencia, no sólo de la conjetura de Bouniakowsky, sino también de una conjetura de Bateman-Horn relativa al número de factores primos de los enteros representados por productos de polinomios irreducibles; véase [10].

Por 15.4 tenemos

19.11. Corolario. Suponemos f primitivo y separable. Sea q tal que las raíces de f se encuentran en el semiplano $\mathrm{Re}(z) \leq q$. Sean k entero ≥ 1, $p > c$ y a primo tales que

$$f(p+q) = a^k c.$$

Suponemos además que alguna de las condiciones siguientes se satisface:

I) $f(q)$ separable y $\mathrm{res}(f, f')/p$;

II) $f'(p+q)$ primo.

Entonces

$$f \text{ es irreducible.}$$

Por 15.5 ocurre

19.12. Corolario. Suponemos f primitivo y separable. Sea q tal que las raíces de f se encuentran en el semiplano $Re(z) \leq q$. Sean k entero ≥ 1 y a primo tales que

$$f(p+q)/d(f) = a^k.$$

Suponemos además que alguna de las condiciones siguientes se satisface:

I) f(q) separable y res $(f,f')/p$;

II) $f'(p+q)$ primo.

Entonces

f es irreducible.

Estableceremos ahora condiciones suficientes para la irreducibilidad total de los polinomios no negativos. Entonces, suponemos nuevamente f no negativo.

De 1.28 y 19.3 deducimos directamente

19.13. Corolario. Sea $q \geq (1/4 + r(f))^{1/2}$. Entonces

f(q+1) primo implica f totalmente irreducible.

Reformulando 19.13, con $p = q + 1$ obtenemos

19.14. Corolario. Sea $p \geq (1/4 + r(f))^{1/2} + 1$. Entonces

f(p) primo implica f totalmente irreducible.

Observamos ahora que en 19.14 no puede ocurrir $p = 2$. Más precisamente, tenemos

$$p \geq (1/4 + r(f))^{1/2} + 1 \quad \text{implica} \quad p > 2.$$

Asimismo, es un hecho

$$p > \text{Sup}\{2,r(f)\} \quad \text{implica} \quad p \geq (1/4 + r(f))^{1/2} + 1.$$

Entonces, resulta

19.15. Proposición. Sea $p > \text{Sup}\{2,r(f)\}$. Entonces

f(p) primo implica f totalmente irreducible.

Probaremos ahora que en 19.15 la restricción $p > \text{Sup}\{2,r(f)\}$ puede suprimirse. En primer lugar, por 1.29 y 19.3 ocurre

19.16. Corolario. Sea $q \geq (1 + r(f))^{1/2} - 1/2$. Entonces

f(q+1) primo implica f totalmente irreducible.

Reformulando 19.16, con $p = q + 1$, obtenemos

19.17. Corolario. Sea $p \geq (1 + r(f))^{1/2} + 1/2$. Entonces

$f(p)$ primo implica f totalmente irreducible.

Por otra parte se tiene

$$p > r(f) \quad \text{implica} \quad p > (1 + r(f))^{1/2} + 1/2.$$

Mejoramos entonces 19.15 como sigue:

19.18. Teorema. Sea $p > r(f)$. Entonces

$f(p)$ primo implica f totalmente irreducible.

19.19. Ejemplo. Consideramos el polinomio $f = X^7 + X^6 + 1$. Tenemos

$$r(f) = 1 \ , \ f(2) = 193.$$

Dado que 193 es primo, f es totalmente irreducible.

20. CONSTRUCCION DE POLINOMIOS IRREDUCIBLES Y TOTALMENTE IRREDUCIBLES

Reformulando 1.28 para $\langle p \rangle$-polinomios de enteros se obtiene

20.1. Corolario. Las raíces de $a_{\langle p \rangle}$ se encuentran en el semiplano

$$Re(z) < (p - 3/4)^{1/2} + 1/2.$$

Entonces, de 19.15 se deduce (A.Cohn; para la instancia típica $p = 10$ véase [7])

20.2. Teorema. Sea $2 < p \leq a$. Entonces

a primo implica $a_{\langle p \rangle}$ totalmente irreducible.

Asimismo, reformulando 1.29 resulta

20.3. Corolario. Las raíces de $a_{\langle p \rangle}$ se encuentran en el semiplano $Re(z) < p^{1/2}$.

Por 19.18 se puede extender 20.2 como sigue:

20.4. **Teorema.** Sea $p \leq a$. Entonces

$$a \text{ primo implica } a_{\langle p \rangle} \text{ totalmente irreducible.}$$

20.5. **Ejemplo.** Dado que a = 9743 es primo, por 20.4 el polinomio

$$a_{\langle 2 \rangle} = X^{13} + X^{10} + X^9 + X^3 + X^2 + X + 1$$

es totalmente irreducible. Con mayor generalidad, los polinomios

$$9743_{\langle k \rangle};\ k = 2, 3, \ldots, 9743$$

son totalmente irreducibles.

20.6. **Nota.** La colección de polinomios totalmente irreducibles con coeficiente principal positivo se denota TI(Z[X]). Entonces el recíproco de 19.8 implica (véase 19.10)

$$TI(Z[X]) = \{b_{\langle k \rangle}(X-j) : b \text{ primo}, k = 2, 3, \ldots, b, j \in Z\}.$$

Por otra parte, la construcción de los irreducibles se reduce mediante traslaciones a la construcción de los irreducibles no negativos. Bastará entonces (véase 6.6), determinar condiciones necesarias y suficientes para que los polinomios $a_{\langle k \rangle};\ k = 2, 3, \ldots, a$ sean irreducibles. Por 6.1 y 20.3, de 16.3 se deriva el criterio siguiente (que puede utilizarse conjuntamente con 6.8):

20.7. **Teorema.** Sean q y p tales que

I) $q \geq k^{1/2}$;

II) $p > (k - 1)(1 + k^{1/2})^{[\log_k a]}$.

Entonces

$$a_{\langle k \rangle} \text{ es irreducible sii } a_{\langle k \rangle}(p + q) \text{ es } \langle p \rangle\text{-irreducible.}$$

20.8. **Ejemplo.** Suponemos a = 93. Sea k = 4. Luego

$$a_{\langle k \rangle} = X^3 + X^2 + 3X + 1.$$

Considerando q = 2 y p = 82 las hipótesis de 20.7 se satisfacen. Ciertamente

$$a_{\langle k \rangle}(p + q) = 614401.$$

Asimismo

$$614401 = (19(30)(57))_{82}.$$

Dado que

$$!614401!_{82} = 97 \text{ (primo)},$$

por 11.2 resulta

$$a_{\langle k\rangle}(p + q) \ \langle p\rangle\text{-irreducible.}$$

Podemos concluir entonces

$$a_{\langle k\rangle} \text{ es irreducible (totalmente irreducible pues } d(a_{\langle k\rangle}) = 1).$$

Observamos ahora que para $j = 1, 2, \ldots$ se tiene

$$2^{j-1} \leq a < 2^j \quad \text{implica} \quad (1 + 2^{1/2})^{[\log_2 a]} < 3^j.$$

Asimismo

$$k \geq 3 \quad \text{implica} \quad (1 + k^{1/2})^{[\log_k a]} < a.$$

Entonces, de 20.7 resulta

20.9. Corolario. Se verifican:

i) Sea j entero positivo. Suponemos $2^{j-1} \leq a < 2^j$. Entonces

$$a_{\langle 2\rangle} \text{ es irreducible sii } a_{\langle 2\rangle}(2 + 3^j) \text{ es } \langle p\rangle\text{-irreducible.}$$

ii) Sea $k \geq 3$. Entonces

$$a_{\langle k\rangle} \text{ es irreducible sii } a_{\langle k\rangle}(k + ka) \text{ es } \langle ka\rangle\text{-irreducible.}$$

Finalmente, complementamos 20.4 como sigue:

20.10. Teorema. Sea $c > 1$. El entero $r(c,p)$ está definido

$$r(c,p) = c \quad \text{o bien} \quad r(c,p) = c + 1$$

de acuerdo con que $p^{1/2}$ sea o no entero. Suponemos p y c tales que

$$((1 + (1 + 4r(c,p))^{1/2})/2)^2 < p \leq ac.$$

Entonces

$$a \text{ primo implica } ((ac)_{\langle p\rangle})_{prim} \text{ irreducible.}$$

Prueba. Suponemos a primo. Sean q el menor entero $\geq p^{1/2}$ y $t = p - q$. Es trivial

$$\text{si } p^{1/2} \text{ es entero entonces } q = p^{1/2}.$$

En consecuencia

$$\text{si } p^{1/2} \text{ es entero entonces } (p - p^{1/2} - c > 0 \quad \text{sii} \quad t > c).$$

Por otra parte

$$\text{si } p^{1/2} \text{ no es entero entonces } q = [p^{1/2}] + 1 < p^{1/2} + 1.$$

Luego

si $p^{1/2}$ no es entero entonces $(p - p^{1/2} - c - 1 > 0$ implica $t > c)$.

En todo caso

$$p - p^{1/2} - r(c,p) > 0 \text{ implica } t > c.$$

Observamos ahora que para w real positivo se tiene

$$w^2 - w - r(c,p) > 0 \text{ sii } w > (1 + (1 + 4r(c,p))^{1/2})/2.$$

Entonces, nuestra hipótesis sobre p y c implica $t > c$. Por 20.3 las raíces de $(ac)_{\langle p \rangle}$ se encuentran en el semiplano $Re(z) \leq q$. La conclusión sigue entonces de 19.5 y la igualdad

$$ac = (ac)_{\langle p \rangle}(t+q).\#$$

20.10. Ejemplos. Convenimos $ac_{\langle p \rangle} = (ac)_{\langle p \rangle}$. Sean $p = 17$ y $c = 11$. Dado que

$$((1 + (1 + 4r(c,p))^{1/2})/2)^2 = 16,$$

las hipótesis de 20.9 se satisfacen si $a \geq 2$. Sea $a = 9973$. Luego

$$ac = 109703,$$

$$ac_{\langle p \rangle} = X^4 + 5X^3 + 5X^2 + 10X + 2.$$

Ciertamente $ac_{\langle p \rangle}$ es primitivo. Puesto que a es primo ocurre $ac_{\langle p \rangle}$ irreducible (totalmente irreducible pues $d(ac_{\langle p \rangle}) = 1$). Análogamente, con $p = 25$, $c = 12$ y $a = 5743$ resulta

$$ac = 74656,$$

$$ac_{\langle p \rangle} = 4X^3 + 19X^2 + 11X + 6.$$

Nuevamente $ac_{\langle p \rangle}$ es primitivo. Dado que a es primo ocurre $ac_{\langle p \rangle}$ irreducible (no totalmente irreducible pues $d(ac_{\langle p \rangle}) = 2$). Por último, consideramos $p = 36$, $c = 20$ y $a = 131$. Se tiene

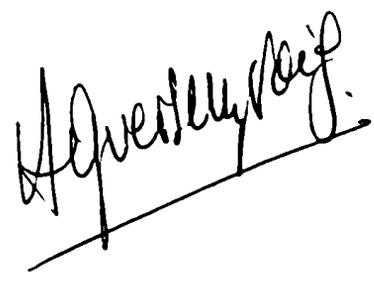
$$ac = 2620,$$

$$ac_{\langle p \rangle} = 2X^2 + 28.$$

Puesto que a es primo, el polinomio

$$(ac_{\langle p \rangle})_{prim} = X^2 + 14$$

es (totalmente) irreducible.



REFERENCIAS

[1] - Hungerford, T. H.; Algebra, Springer-Verlag, pp. 166-167.

[2] - Dickson, L. E.;History of the theory of numbers, Chelsea, Vol.I, pp. 12, 15, 332-334.

[3] - Cohn, P. M.; Algebra, Wiley & Sons, Vol. 1, pp. 175-178.

[4] - Marden, M.; The geometry of the zeros of a polynomial in a complex variable, American Mathematical Society, Mathematical Surveys, Number III, pp. 95-103, 126-158.

[5] - Dieudonne, J.; Cálculo infinitesimal, Omega, pp. 68, 70.

[6] - Faadieev, D. y Sominski, I.; Problemas de álgebra superior, Mir, pp. 94-95, 100-101.

[7] - Pólya, G.-Szego, G.; Problems and theorems in analysis, Springer-Verlag, Vol. I, Pt. III, pp. 106-107; Pt. VIII, p. 133.

[8] - Gantmacher, F. R.; The theory of matrices, Chelsea, Vol. II, pp. 172-250.

[9] - Mignotte, M.; An inequality about factors of polynomials, Math. Comp., pp. 1153-1157.

[10]- Shanks, D.; Solved and unsolved problems in number theory, Chelsea, pp. 3, 25, 193-200, 220-221.

[11]- Knuth, D. E.; The art of computer programming, Addison Wesley, Vol. 2, Seminumerical algorithms, pp. 364-389, 420-441.

[12]- Pomerance, C.; Recents developments in primality testing, The Mathemathical intelligencer, Vol. 3, pp. 97-105.

[13]- Pomerance, C.; The search for primes, Scientific American, Number 247, pp. 136-147.

[14]- Adleman, L. M.,Pomerance, C. and Rumely, R. S.; On distinguishing prime numbers from composite numbers, Annals of Mathematics, Volume 117, pp. 173-206.

[15]- Rumely, R.; Recents advances in primality testing, Notices of the American Mathematical Society, Volume 30, pp. 475-477.

[16]- Guy, R. K.; How to factor a number, Proceedings of the Fifth Manitoba Conference on Numerical Mathematics, Utilitas, Winnepeg, Manitoba, pp. 49-89.

[17]- Archibald, R. G.; An introduction to the theory of numbers, Merrill Mathematics Series, pp. 73-75.

[18]- Koblitz, N.; p-adic Numbers, p-adic Analysis & Zeta Functions, Springer-Verlag, p.13.

[19]- Guersenzvaig, N. H.; Caracterización residual de los divisores de polinomios con coeficientes enteros, manuscrito no publicado.

[20]- Guersenzvaig, N. H.; Caracterizaciones de los divisores de polinomios en varias indeterminadas con coeficientes enteros, manuscrito no publicado.

[21]- Guersenzvaig, N. H.; Caracterizaciones de los divisores de polinomios en varias indeterminadas, manuscrito no publicado.

[22]- Guersenzvaig, N. H,; Caracterizaciones de los divisores de polinomios, manuscrito en preparación.

[23]- Brillhart, J.; Note on irreductibility testing, Math. Comp., pp. 1379-1381.

[24]- VIII Seminario nacional de matemática (1986), Universidad Nacional de Córdoba, República Argentina., Vol. II, p. 85.

[25]- Apostol, T. M.; Introduction to Analytic Number Theory, Springer-Verlag, Chapter 7.

NOTACIONES ESPECIALES