Revista Colombiana de Estadística
Nº 12 - Diciembre - 1985

DESCOMPOSICION DE UN POLINOMIO SOBRE Z_p (CUERPO DE LOS ENTEROS MODULO EL PRIMO P) EN SUS FACTORES IRREDUCIBLES MEDIANTE UN COMPUTADOR

Rubén Darío Nieto C.
Depto. de Matemáticas
Universidad del Valle

Introducción.

La relación entre computadores y matemática pura va adquiriendo cada día más importancia. La construcción de un programa de computador a partir de un conjunto de instrucciones básicas es bastante similar a la construcción de una demostración a partir de un conjunto de axiomas. Tanto números como símbolos pueden ser manipula-

dos por un computador lo que ha permitido la creación de nuevos algoritmos de propósito general (Pavelle R. 1981) que pueden hacerse cargo de una amplia variedad de trabajo matemático rutinario y resolver problemas que se hacen inmanejables de otra manera.

De las afirmaciones anteriores (Knuth D.E. 1981, Pavelle R. 1981) se desprende que la conexion entre computadores y matemática es más íntima y profunda de lo que generalmente se cree.

Por otra parte la existencia hoy en día de computadores de características impresionantes, aunado a la posibilidad de acceder a ellos, son de por sí un desafío a la utilización de éstos dentro del mundo de la matemática, a tal punto que existen ya campos de investigación como "Algebra Computacional" (Pavelle R. 1981) que se mueven en una mezcla de Algebra y Ciencias de la Computación.

Dentro de esta línea nos proponemos en el presente artículo explicar las bases matemáticas del programa "FACMOPRI" que introducido a un computador (no muy sofisticado) logra que de un polinomio dado T de grado GT, éste obtenga todos sus factores irreducibles junto con sus multiplicidades sobre el cuerpo $K = Z_p$ de ente-

ros módulo el primo p (Childs L. 1979).

Nota.

1) En el presente artículo trabajaremos exclusivamente con polinomios cuyos coeficientes están todos en el cuerpo $K = Z_p$.

2) Para significar que un polinomio F divide al polinomio T escribiremos $F|T$ y si F no divide a T escribiremos $F \nmid T$.

3) El teorema pequeño de Fermat (Childs L. 1979) afirma la siguiente igualdad de polinomios:

$$h_0+h_1x^p+h_2x^{2p}+\ldots+h_mx^{mp} = (h_0+h_1x+h_2x^2+\ldots+h_mx^m)^p$$

4) A veces la derivada de un polinomio F la denotaremos con F'.

Observación.

1) El polinomio $a_0+a_1x+a_2x^2+\ldots+a_nx^n$ de coeficiente principal a_n lo podemos representar en un computador como el arreglo (Tremblay J.P. 1982) $A = (a_0, a_1, a_2, \ldots, a_n)$ tomando $a_i = A(i)$ para $i = 0, 1, 2, \ldots, n$ y además GA = grado de $A = n$.

2) El polinomio $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ de grado n lo podemos también representar como el arreglo $A = (a_n, a_{n-1}, \ldots, a_0)$ tomando $a_{n-i} = A(i)$, para $i = 0, 1, 2, \ldots, n$ y además $GA = n$. Obsérvese que en esta segunda representación el coeficiente principal es $a_n = A(0)$ y el coeficiente constante es $a_0 = A(GA)$.

Nota.

En los diagramas de flujo (Tremnaly, J.P.; 1982) que sean utilizados adoptaremos los siguientes convenios:

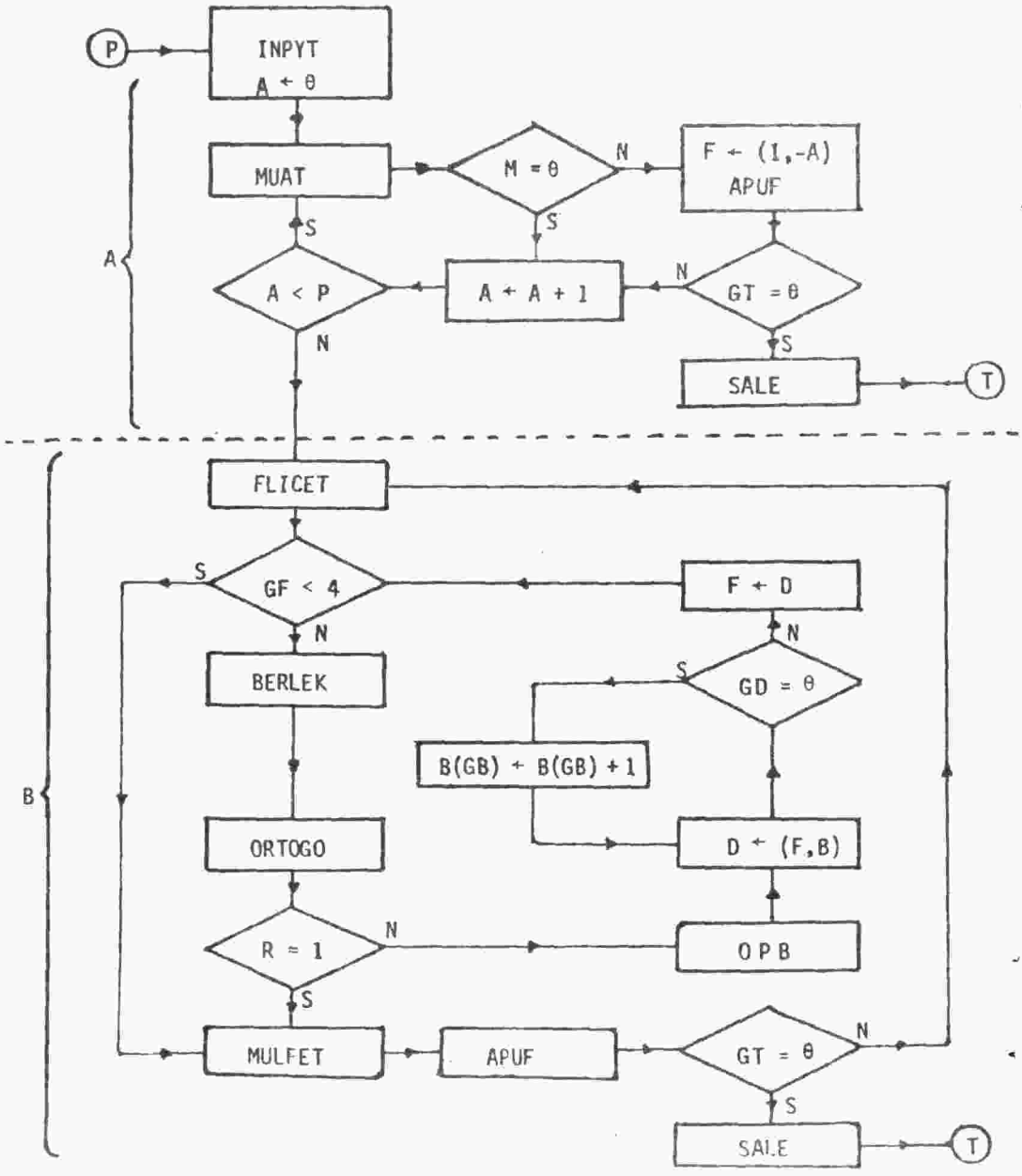
1) Los símbolos Ⓟ y Ⓣ se usarán para indicar donde principia y donde termina respectivamente un diagrama.

2) Se usará el símbolo "←" para indicar la operación de asignación (Tremblay J.P. 1982).

3) Para indicar una "bifurcación" (Tremblay J.P. 1982) se usará un rombo junto con las letras *S* y *N* (*S* significa "Si", *N* significa "No").

FACMOPRI.

El diagrama de flujo del mencionado programa "FACMOPRI" es el siguiente:


P
INPYT
A ← θ
MUAT
M = θ
N
F ← (1,-A)
APUF
S
S
A
A < P
A ← A + 1
N
GT = θ
N
S
SALE
T
N
FLICET
S
GF < 4
F ← D
N
N
BERLEK
S
GD = θ
B(GB) ← B(GB) + 1
B
ORTOGO
D ← (F,B)
R = 1
N
OPB
S
MULFET
APUF
GT = θ
N
S
SALE
T

Llamaremos polinomio T, polinomio de trabajo, a aquel del cual se están buscando sus factores irreducibles F y sus respectivas multiplicidades M. Como se puede observar "FACMOPRI" está dividido en las partes A y B. La parte A se encarga de los factores lineales y la parte B del resto de factores irreducibles.

P A R T E A

I) El subprograma "INPYT" introduce al computador el primo p, el grado $GT = FU$ del polinomio de trabajo inicial T y los coeficientes de T (aquí la longitud de la palabra del computador entra a limitar el tamaño de los números a introducir).

II) El subprograma "MUAT" obtiene la multiplicidad M del factor $X-A = (1,-A)$ en T y el polinomio Q tal que $T = (X-A)^M Q$, donde $X-A$ no divide a Q, dejando a Q como nuevo polinomio de trabajo T. "MUAT" se basa esencialmente en la muy conocida división sintética de polinomios.

III) Si es la primera vez que se pasa por "APUF" éste inicializa NF el número de factores irreducibles, ésto es, asigna 0 a NF y además asigna a U la matriz nula $0[FU, FU+3]$ de FU filas y $FU+3$ columnas, en donde FU es el grado del polinomio

de trabajo inicial (aquí la memoria del computador entra a limitar el número FU y por tanto el grado del polinonio de trabajo inicial).

Por cada paso por "APUF" (apunta factores) se aumenta NF en una unidad y se apunta el factor irreducible F así:

a) En $U(NF,1)$ la multiplicidad M.

b) En $U(NF,2)$ el grado GF.

c) En el resto de la fila NF de U se apuntan los coeficientes de F después de haberlos dividido módulo el primo p, por el coeficiente principal de F y en el caso de que haya algún coeficiente negativo se le suma p tantas veces cuantas sea necesario para volverlo positivo.

IV) "SALE" obtiene M = maximal $\{U(i,2)+3$ en donde $i = 1,2,\ldots,NF\}$. (Recordemos que $U(i,2)$ es el grado del i-simo polinomio irreducible F) tomando luego $FA = NF$, $CA = M$ y asignando a A la matriz nula $\theta[FA,CA]$ de FA filas y CA columnas.

Por último toma $A(i,j) = U(i,j)$ para $j = 1, 2,\ldots,CA$ para $i = 1,2,\ldots,FA$.

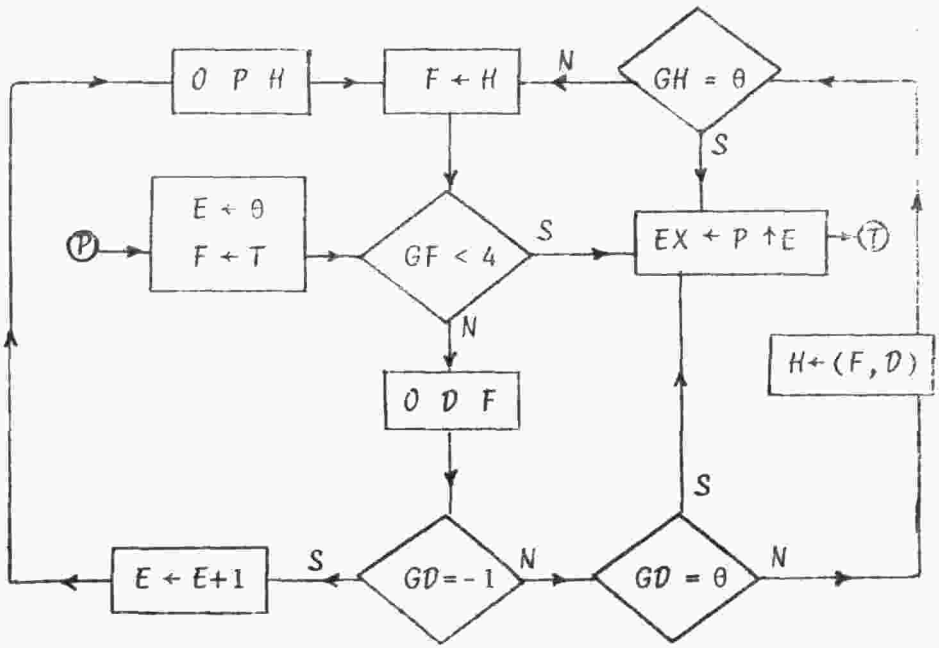
De esta manera los distintos factores irreducibles del polinomio de trabajo inicial y sus respectivas multiplicidades se pueden leer apro

piadamente en la matriz A de FA filas y CA columnas.

P A R T E B

I) El subprograma "FLICET" extrae del polinomio de trabajo T un factor F no constante, libre de cuadrados (no necesariamente irreducible). Arroja también el entero no negativo EX teniéndose que existe un polinomio, digamos Q, tal que $T = F^{EX}Q$ en donde F puede dividir a Q. Además no cambia a T.

El subprograma "FLICET" luce así:



Nota.

1) $P\uparrow E$ es lo mismo que P^E.

2) $GD = -1$ significa que el polinonio D es el polinomio nulo.

El teorema que viene a continuación explica la presencia del nodo de decisión $GF < 4$ en el anterior diagrama.

Teorema 1. *Sea F un polinomio no constante y que no admite factores lineales. Si F es de grado menor que cuatro entonces F es irreducible (y por tanto libre de cuadrados).*

El siguiente teorema explica la presencia en "FLICET" de los subprogramas "ODF" que obtiene la derivada D del polinomio F y "OPH" que obtiene el polinomio H. Explica también la presencia de los nodos de decisión $GD = -1$ y de asignación $E \leftarrow E + 1$.

Teorema 2. *Sea F un polinonio no constante. Su derivada D es nula ($GD = -1$) si y sólo si existe otro polinomio H no constante tal que $F = H^p$.*

Demostración. (Childs L. 1979).

Corolario. *Si F es un polinomio irreducible su derivada D nunca es nula.*

Demostración. Si D es nula entonces por el teorema anterior $F = H^p$ con H no constante lo cual implica que F no es irreducible.

Teorema 3. *Sea F un polinomio no constante D su correspondiente derivada $H = F,D$ el máximo común divisor de F y D. Si $F = A^a B^b C^c \ldots$ es la descomposición de F en sus distintos factores irreducibles $A, B, C, \ldots$ entonces la descomposición de H en sus distintos factores irreducibles viene dada por $H = A^x B^y C^z \ldots$ en donde*

$$x = \begin{cases} a & si \quad p \mid a \\ a-1 & si \quad p \nmid a \end{cases}$$

y similarmente para los otros exponentes $y, z, \ldots$

Ejemplo 1. Si $p = 3$ y $F = A^8 B^6 C^3 E^2$ entonces $H = A^7 B^6 C^3 E$.

Demostración. Miremos el caso en que F tiene sólo dos factores irreducibles diferentes. El caso general se demuestra usando las mismas ideas desarrolladas en este caso particular.

Tenemos $F = A^a B^b$ y así:

$$D = aA^{a-1} A' B^b + bB^{b-1} B' A^a$$

Supongamos que $A^a \mid D$.

Concluímos que $A^a | aA^{a-} A'B^b$ y así $A | aA'B^b$. Puesto que A es irreducible debe dividir a alguno de los tres factores a, A', B^b. Como A' es de menor grado que A vemos que si $A | A'$ entonces A' debe ser nulo contradiciendo el corolario anterior.

Por otra parte si $A | B^b$ entonces $A | B$ lo que implica que A es asociado de B (Tremblay, J.P.; 1982) por tratarse de irreducibles, contradiciendo la hipótesis.

Concluímos que $A | a$ y como A es de grado mayor que a debe tenerse $a = \theta$ y por tanto $p | a$.

Así que:

1) Si $p \nmid a$ entonces A^{a-1} es la potencia de A mayor exponente que divide tanto a F como $\mathcal{D}$.

2) Si $p | a$ entonces $aA^{a-1}A'B^b = \theta$ con lo que $\mathcal{D} = bB^{b-1}B'A^a$ y así A^a es la potencia de A de mayor exponente que divide tanto a F como a $\mathcal{D}$.

Como el máximo común divisor se forma de los factores irreducibles comunes con su mayor exponente, hemos demostrado el teorema para este caso particular.

El Corolario que viene a continuación expli

ca la presencia en "FLICET" de los nodos de decisión $GD = 0$ y $GH = 0$ y además la del subprograma $H \leftarrow (F,D)$ que obtiene el máximo común divisor H de los polinomios F y D (mediante el "Algoritmo de Euclides" (Childs, L.; 1979)).

Corolario. *Sea F un polinomio no constante. F es libre de cuadrados si y sólo si $H = (F,D)$ el máximo comun divisor de F y su derivada D es constante.*

Demostración. (Necesidad).

Como F es libre de cuadrados la descomposición de F en sus distintos factores irreducibles es $F = A^a B^b C^c \ldots$ en donde $a = b = c = \ldots = 1$ por el teorema anterior tenemos

$H = A^x B^y C^z \ldots$ donde $x = y = z = \ldots = 0$ puesto que $p \nmid 1$.

Concluímos que H es constante.

(Suficiencia).

Si F no es libre de cuadrados entonces $F = A^a B^b C^c \ldots$ donde $A, B, C, \ldots$ son irreducibles y alguno de los exponentes, digamos a, es mayor que uno.

Por el teorema anterior deducimos que $H =$

$A^x B^y C^z \ldots$ donde $x > 0$. Concluímos que H no es constante.

II) El subprograma "BERLEK" obtiene la matriz de Berlekamp asociada al polinomio F, que se define a continuación.

Nota.

Los polinomios de grado no mayor que $V \geq 0$ los podemos mirar como arreglos de dimensión $V+1$, por ejemplo si $V = 5$, el polinomio $H = 2 + 3x + x^2 + 2x^3$ lo podemos mirar como el arreglo $H = (2,3,1,2,0,0)$ con $H(0) = 2$, $H(1) = 3$, $H(2) = 1$, $H(3) = 2$, $H(4) = 0$, $H(5) = 0$.

Por tanto el polinomio X^j con $j \leq V$ es el arreglo E_j definido así:

$$E_j(i) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Así las cosas, un polinomio H de grado no mayor que V lo podemos también tomar de la siguiente manera:

$$H = \sum_{i=0}^{V} H(i) X^i = \sum_{i=0}^{V} H(i) E_i$$

Definición. Sea F un polinomio de grado $GF = V+1$

con $V \geq 0$.

a) Al conjunto C de todos los polinomios B de grado no mayor que V y tales que $F \mid B^p - B$ lo llamaremos "conjunto de Berlekamp asociado a F".

b) A la matriz cuadrada A de orden $V+1$, formada de la manera que a continuación se describe, la llamaremos "Matriz de Berlekamp asociada al polinomio F".

1) Para $j = 0,1,2,\ldots,V$ a cada polinomio $D_j = X^i$ donde $i = j \times p$, apliquemos el algorítmo de la división para obtener el polinomio cociente Q_j y el polinomio residuo H_j tales que $D_j = F \times Q_j + H_j$ donde $H_j = 0$ ó $GH_j < GF$.

Si $GH_j < GF = V+1$ vemos que $GH_j < V$ con lo cual podemos, de acuerdo a la nota anterior, tomar H_j (incluído el caso $H_j = 0$) como un arreglo de dimensión $V+1$ para $j = 0,1,2,\ldots,V$.

2) Formemos la matriz cuadrada M de orden $V+1$ colocando a H_j como la j-sima columna de M para $j = 0,1,2,\ldots,V$, esto es:

$$M(i,j) = H_j(i)$$

para $j = 0,1,2,\ldots,V$: para $i = 0,1,2,\ldots,V$.

3) Por último establezcamos la mencionada matriz

A de Berlejamp restándole a la matriz A la matriz idéntica de orden $V+1$, es decir:

$$A(i,j) = M(i,j) - \delta_{ij} = H_j(i) - E_j(i) \therefore$$

$$A(i,j) = H_j(i) - E_j(i)$$

para $j = 0,1,2,\ldots,V$: para $i = 0,1,2,\ldots,V$.

Ejemplo 2. Sea $p = 3$, $F = 2+x+2x^2+x^3+x^4$. GF es entonces 4 y $V = 3$. Realizando las mencionadas divisiones obtenemos:

$$H_0 = x^0 = 1 = (1,0,0,0)$$
$$H_1 = x^3 = (0,0,0,1)$$
$$H_2 = 2+x^2+2x^3 = (2,0,1,2)$$
$$H_3 = 2x+2x^3 = (0,2,0,2)$$

$$M = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 \end{pmatrix} \qquad A = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

El conjunto C es

$$C = \{0,1,2,2x+x^3,1+2x+x^3,2+2x+x^3,x+2x^3,$$
$$1+x+2x^3,2+2x+2x^3\}.$$

A partir de A mediante el proceso de Gauss-

Jordan (Childs, L.; 1979) podemos obtener la matriz H escalonada reducida por filas correspondiente a la matriz A juntamente con su rango X, su nulidad Y y las funciones L y D definidas así:

a) $L(j)$ = posición de la j-ésima columna independiente de H (para $j = 1,2,\ldots,X$).

b) $D(j)$ = posición de la j-ésima columna dependiente de H (para $j = 1,2,\ldots,Y$).

En el ejemplo 2: $$H = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$X = 2, \quad Y = 2.$

$L(1) = 2, \quad L(2) = 3; \quad D(1) = 1, \quad D(2) = 4.$

Tomemos ahora $R = Y$.

A partir de H podemos entonces obtener una matriz $O = A^{\perp}$, del mismo número de columnas que A, que llamaremos matriz ortogonal a A, y que definiremos así:

a) Si $R = 0$ entonces O tiene una sola fila nula.

b) Si $R \neq 0$ entonces O tiene R filas formadas así:

i) $O(i,D(j)) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$

ii) Si $X \neq 0$ entonces

$$O(i,L(j)) = -H(j,D(i))$$

para $i = 1,2,\ldots,R$; para $j = 1,2,\ldots,X$.

Se puede demostrar entonces el siguiente Teorema:

Teorema 4, 1) *Las R filas de la matriz* $O = A^{\perp}$ *son linealmente independientes (a menos que R sea cero).*

Las R filas de la matriz $O = A^{\perp}$ *son ortogonales a las filas de la matriz* A.

Además se puede establecer también el siguiente corolario.

Corolario. 1) *El espacio nulo* $n(A)$ *de la matriz* A *es el espacio fila* $f(O)$ *de la matriz* O.

2) *El espacio fila* $f(A)$ *de la matriz* A *es el espacio nulo* $n(O)$ *de la matriz* O.

III) El subprograma "ORTOGO" obtiene una matriz O ortogonal a la matriz A de Berlekamp asociada al polinomio F.

En el ejemplo 2 los elementos de C se encontraton utilizando el siguiente teorema:

Teorema 5. *Sea* F *un polinomio de grado* GF = V+1 *con* V ≥ 0. *Sea* O *una matriz ortogonal a la matriz* A *de Berlekamp aosicada al polinomio* F *entonces*

$$C = \mathcal{G}(O)$$

en donde C *es el conjunto de Berlekamp asociado al polinomio* F *y* $\mathcal{G}(O)$ *es el espacio fila de la matriz* O.

Demostración. Tanto el polinomio nulo como los polinomios constantes están en C puesto que por el teorema pequeño de Fermat $a^p = a$ para todo $a \in K = Z_p$ y por tanto $F | a^p - a$.

La primera columna de A es nula así que comando a $E_0 = (1,0,0,\ldots,0)$ como columna obtenemos $AE_0 = 0$ lo que muestra que el arreglo E_0 está en $n(A)$ el espacio nulo de A. Como $\mathcal{G}(O) = n(A)$, E_0 está en $\mathcal{G}(O)$. Deducimos entonces que el polinomio nulo y los polinomios constantes están en $\mathcal{G}(O)$.

Por otra parte sea

$$\sum_{j=0}^{V} B(j)X^j = \sum_{j=0}^{V} B(j)E_j$$

un polinomio no nulo, no constante y de grado no mayor que V.

Por el pequeño teorema de Fermat tenemos:

$$B^p = \sum_{j=0}^{V} B(j)X^{pj} = \sum_{j=0}^{V} B(j)X^{j} = \sum_{j=0}^{V} B(j)D_j$$

$$= \sum_{j=0}^{V} B(j)(FQ_j + H_j) \quad \therefore$$

$$B^p - B = \sum_{j=0}^{V} B(j)(FQ_j + H_j) - \sum_{j=0}^{V} B(j)E_j$$

$$= \sum_{j=0}^{V} B(j)FQ_j + \sum_{j=0}^{V} B(j)(H_j - E_j)$$

Tomando $Q = \sum_{j=0}^{V} B(j)Q_j$ vemos que

$$B^p - B = FQ + \sum_{j=0}^{V} B(j)(H_j - E_j)$$

$$= FQ + \sum_{j=0}^{V} B(j) \sum_{i=0}^{V} (H_j - E_j)(i)E_j$$

por la nota anterior.

Ahora:

$$B^p - B = FQ + \sum_{j=0}^{V} B(j) \sum_{i=0}^{V} (H_j(i) - E_j(i))E_i$$

$$= FQ + \sum_{j=0}^{V} B(j) \sum_{i=0}^{V} A(i,j)E_i$$

$$= FQ + \sum_{j=0}^{V} \left(\sum_{j=0}^{V} A(i,j)B(j) \right) E_i .$$

Deducimos que:

$$B^p - B = FQ + \sum_{i=0}^{V} S_i E_i = FQ + \sum_{i=0}^{V} S_i X^i$$

donde $S_i = \sum_{j=0}^{V} A(i,j)B(j)$ para $i = 0,1,2,\ldots,V$.

Concluímos entonces que F divide a $B^p - B$ si y sólo si F divide a $\sum_{i=0}^{V} S_i X^i$ que tienem cuando más grado V mientras que F tiene grado $V+1$, es decir,

$$F \mid B^p - B \Leftrightarrow \sum_{i=0}^{V} S_i X^i = 0$$

$$\Leftrightarrow S_i = 0 \text{ para } i = 0,1,2,\ldots,V$$

$$\Leftrightarrow \sum_{j=0}^{V} A(i,j)B(j) = 0 \text{ para } i = \ ,1,2,\ldots,$$

$$\Leftrightarrow B \in n(A) = \mathcal{G}(0).$$

Ejemplo 3. Refiriéndonos al ejemplo 2 se obtiene

$$0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix} \quad \text{y así:}$$

$\mathcal{G}(0)$ = espacio generado por el conjunto F_1, F_2

sobre $K = Z_3 = \{0,1,2\}$ donde $F_1 = (1,0,0,0)$, $F_2 = (0,2,0,1)$. Tenemos entonces:

$$C = \mathcal{G}(0) = \{xF_1 + yF_2 : x,y \in K\}$$

IV) Consideremos el rango R de la matriz ortogonal O. Como vimos $E_0 = (1,0,0,\ldots,0)$ está siempre en $\mathcal{G}(0)$ de manera que si $R \neq 1$ entonces la matriz O debe tener al menos una fila, digamos S, que no es múltiplo escalar de E_0.

El subprograma "OPB" de "FACMOPRI" asigna a B la fila S de menor grado.

Lema 1. *Para todo polinomio* B *sobre* $K = Z_p$ *se cumple:*

$$B^p - B = B(B+1)(B+2)\ldots(B+p-1) = \prod_{r=0}^{p-1} B+r$$

Demostración. (Childs, L.; 1979).

V) El siguiente teorema explica la presencia en "FACMOPRI" del subprograma $D \leftarrow (F,B)$, de los nodos de asignación $B(GB) \leftarrow B(GB)+1$, $F \leftarrow D$ y del nodo de decisión $GD = 0$.

Teorema 6. *Sea* F *un polinomio de grado* $GF = V+1$ *con* $V \geq 0$. *Sea* C *el conjunto de Berlekamp asociado al polinomio* F. *Para todo* B *elemento de* C

no nulo y no constante se cumple:

1) $F = \mathcal{D}_0\mathcal{D}_1\ldots\mathcal{D}_{p-1}$ donde $\mathcal{D}_r = (F, B+r)$ para $r = 0,1,2,\ldots,p-1$.

2) $G\mathcal{D}_r < GF$ para $r = 0,1,2,\ldots,p-1$.

3) $G\mathcal{D}_r \neq 0$ para algún r en $\{0,1,2,\ldots,p-1\}$.

Demostración. (Childs, L.; 1979).

Lema 2. *Sean F y C como en el teorema anterior con F libre de cuadrados. Sea N el número de distintos factores irreducibles en que se descompone F sobre el cuerpo* $K = Z_p$ *entonces:*

$$|C| = |K^N|$$

esto es: el número de elementos del conjunto C es igual al número de elementos del conjunto K^N.

Demostración. Sea $F = F_1F_2\ldots F_N$ la descomposición de F en sus distintos factores irreducibles Nos proponemos establecer una función inyectiva L de C sobre K^N.

Fijemos un B elemento de C y sea i un elemento cualquiera de $\{1,2,\ldots,N\}$.

Por el teorema anterior $F = \mathcal{D}_0\mathcal{D}_1\ldots\mathcal{D}_{p-1}$ con $\mathcal{D}_r = (F, B+r)$ para $r = 0,1,2,\ldots,p-1$.

Puesto que F_i divide a F entonces F_i (que es irreducible) debe dividir a algún $\mathcal{D}_r$ y sólo uno porque si también $F_i | \mathcal{D}_s$ entonces F_i divide a $B+r$ y a $B+s$ con lo que $F_i | B+r-(B+s) = r-s$ deduciéndose que $r-s = 0$ o sea que $r = s$.

Así pues fijado un B elemento de C se establece una función L_B del conjunto $\{1,2,\ldots,N\}$ en K definida por $L_B(i) = r$ donde r es tal que $F_i | (F, B+r)$.

Es entonces de sentido común definir a L así:

$$L(B) = (L_B(1), L_B(2), \ldots, L_B(N)).$$

Primero. La función L es inyectiva.

Si $L(B) = L(H)$ entonces $L_B(i) = L_H(i)$ para $i = 1,2,\ldots,N$ con lo cual si fijamos un i y tomamos $r = L_B(i) = L_H(i)$ entonces $F_i | (F, B+r)$ y también $F_i | (F, H+r)$ deduciéndose que F_i divide a ambos $B+r$ y $H+r$. Concluímos entonces que $F_i | B+r-(H+r)$ o sea que $F_i | B-H$. Este razonamiento es válido para $i = 1,2,\ldots,N$. Como los F_i son todos irreducibles, deducimos que $F | B-H$. Pero $GF > G(B-H)$ y por ello necesariamente se tiene $B-H = 0$ o sea $B = H$.

Segundo. La función L es sobreyectiva.

Sea $(S_1, S_2, \ldots, S_N)$ un elemento cualquiera de K^N ($S_i \in K$ para $i = 1,2,\ldots,N$). Por teorema del residuo chino para polinomios (Childs, L.; 1979) existe un polinomio B con $GB \leq V$ tal que $B \equiv -S_i \bmod F_i$ para $i = 1,2,\ldots,N$.

Se tiene entonces que $F_i \mid B+S_i$ para $i = 1,2,\ldots,N$.

Por otra parte si fijamos un i tenemos

$$B + S_i \mid \prod_{r=0}^{p-1} B + r$$

ya que $S_i \in K$ y los elementos de K son $0,1,2,\ldots p-1$.

Como $\prod_{r=0}^{p-1} B + r = B^p - B$, por Lema 1, deducimos que $F_i \mid B^p - B$ para $i = 1,2,\ldots,N$ y puesto que los F_i son todos irreducibles concluímos que $F \mid B^p - B$, es decir que B está en el conjunto C.

Ahora como $F_i \mid B+S_i$ se tiene que $F_i \mid (F, B+S_i)$ o sea $L_B(i) = S_i$ para $i = 1,2,\ldots,N$. Esto es:

$$L(B) = (S_1, S_2, \ldots, S_N).$$

Teorema 7. *Sean F, C y N como en el Lema 2 y sea O como en el Teorema 5 entonces N es el rango R de la matriz O.*

Demostración. Como K tiene p elementos tenemos

que:

a) K^N tiene p^N elementos.

b) $\mathcal{N}(0)$ tiene p^R elementos.

Además por el Teorema 5 se tiene $C = \mathcal{N}(0)$ y por el Lema 3 $|C| = |K^N|$.

Deducimos entonces que $|\mathcal{N}(0)| = |K^N|$ ésto es: $p^R = p^N$ y por consiguiente $R = N$.

Pregunta. ¿Es posible que sea R igual a uno sin que el polinomio F sea irreducible?

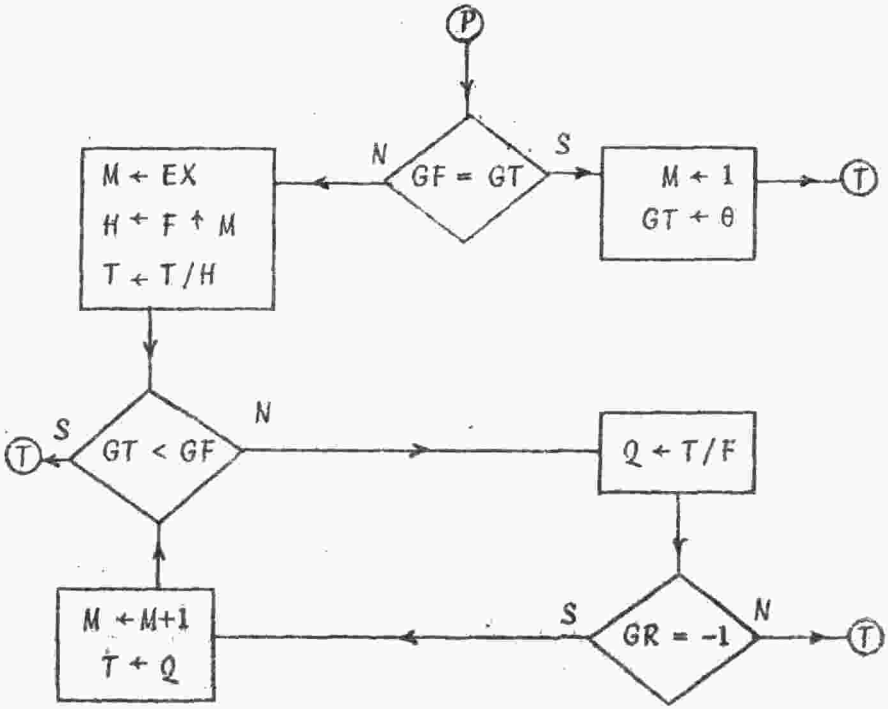
Respuesta. Tomemos $p = 3$ y $F = X^2$ entonces $M = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $\therefore$ $A = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}$ $\therefore$ $0 = (1,0)$ y así $R = 1$ sin que F sea irreducible, pero evidentemente tal cosa no sucedería si F fuése libre de cuadrados.

El siguiente corolario acaba de explicar la presencia del nodo de decisión $R = 1$ en "FACMOPRI".

Corolario. *Sea F un polinomio no constante y libre de cuadrados. Sea R el rango de la matriz (R es el número de filas de Q puesto que las filas de Q son independientes) ortogonal a la matriz A de Berlekamp asociada al polinomio F entonces F es irreducible si y sólo si R es igual a uno.*

VI) El subprograma "MULFET" obtiene la multiplicidad M de F en T y el polinomio Q tal que $T = F^M Q$ donde F no divide a Q, dejando luego a Q como nuevo polinomio de trabajo T.

El subprograma "MULFET" luce así:



Nota.

1) Recordemos que por "FLICET" se tiene que $F^{EX} Q = T$ en donde F puede dividir a Q.

2) Para elevar F a la potencia $M = EX$ se puede

utilizar el teorema pequeño de Fermat ya que es una potencia del primo *p*.

3) En el algoritmo de la división de polinomios con *T/F* significamos el cociente y con *GR* el grado del residuo de dividir a *T* entre *F*. (*GR* = -1 si el residuo es nulo).

* *

BIBLIOGRAFIA

Childs, L., *A concrete Introduction to Higher Algebra*. Springer Verlag. 1979.

Knuth, D.E., *El arte de programar los ordenadores (computadores)*, Vol.1 Algoritmos Fundamentales. Edit. Reverté, S.A., 1980.

Knuth, D.E., *The art of computer programming*, Vol.2 Seminumerical algorthms, Addison Wesley, Reading, Second edition 1981.

Pavelle, R., *Computer Algebra*. Scientific American, Diciembre 1981. Vol. 245.

Tremblay, J.P., *Introducción a la Ciencia de los Computadores. Enfoque Algorítmico*. McGraw-Hill. 1982.

* *