SOBRE A PARIDADE DOS COEFICIENTES DE POLINÔMIOS CUJAS RAÍZES SÃO INTEIRAS

Marcelo POLEZZI[1]
Trajano Pires da NÓBREGA NETO[2]

▪ RESUMO: Considere um polinômio $f(x) = (x - x_1) \cdots (x - x_n)$, onde $x_1, \ldots, x_n \in \mathbb{Z}$. Neste artigo apresentaremos três resultados que relacionam o número de coeficientes pares/ímpares de $f(x)$ com o número de raízes pares/ímpares de $f(x)$. Esses resultados estão intimamente ligados às *relações de Girard* (devidas ao matemático franco-flamengo Albert Girard, 1595-1632) e a um critério de divisibilidade para coeficientes binomiais.

▪ PALAVRAS-CHAVE: Polinômios com raízes e coeficientes inteiros; relações de Girard; critério de divisibilidade para coeficientes binomiais.

1 Introdução

Seja $f(x) = \prod_{i=1}^{n}(x - x_i)$, onde $x_1, \ldots, x_n \in \mathbb{Z}$. Escreva $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ e considere os seguintes conjuntos:

$$RP(f) = \{1 \leq j \leq n \ / x_j \text{ é par } \}, \ RI(f) = \{1 \leq j \leq n \ / x_j \text{ é ímpar } \},$$
$$CP(f) = \{0 \leq j \leq n-1 \ / a_j \text{ é par } \}, \ CI(f) = \{0 \leq j \leq n-1 \ / a_j \text{ é ímpar } \}.$$

Com isso, temos os seguintes resultados:

Teorema 1. $| \ CI(f) \ |$ é ímpar $\Leftrightarrow RI(f) \neq \emptyset$.

Teorema 2. Seja $k \in \mathbb{N}, \ 0 < k \leq n$. Então,

$$CP(f) = \{0, \ldots, k-1\} \Leftrightarrow |RP(f)| = k \ \text{ e } \ n - k = |RI(f)| = 2^t - 1.$$

[1]Universidade Estadual de Mato Grosso do Sul - UEMS, CEP 79540-000, Cassilândia, MS, Brasil. E-mail:*mpolezzi@terra.com.br*
[2]Departamento de Matemática, Universidade Estadual Paulista - UNESP, CEP 15054-000, São José do Rio Preto, SP, Brasil. E-mail:*trajano@ibilce.unesp.br*

Teorema 3. Suponha que $RP(f) = \emptyset$. Então, para quaisquer inteiros não-negativos j, k e l, temos:

(i) Se $n = 2^k(2^j - 1)$, então $|CI(f)| = 2^j - 1$. Além disso, se $n > 6$ for um número perfeito par, então $|CI(f)|$ será primo e $|CP(f)|$ será divisísel por $3|CI(f)|$. (Se $n = 6$, $|CI(f)| = 3 = |CP(f)|$).

(ii) Se $n = 2^{k+2}(2^{j+1} + 1) - 1$, então $|CI(f)| = 2^{k+3} - 1$

(iii) Se $n = 2^{k+2}(2^{l+j} + 2^l - 1) + 1$ ou $n = 2\{2^l(2^{j+k+1} + 2^k + 1) - 1\}$, então $|CI(f)| = 2^{l+2} - 1$

2 Prova do Teorema 1

Para demonstrarmos o Teorema 1, usaremos o seguinte fato elementar:

Lema 1. *Seja* $m \in \mathbb{N}$, *e considere* $S = \left\{ 1 \leq j \leq m \;\middle/\; \binom{m}{j} \text{ é ímpar} \right\}$. *Então,* $|S|$ *é ímpar.*

Prova: Se $|S|$ for par, então $\sum_{j \in S} \binom{m}{j}$ será par. Por conseguinte, $\sum_{j=1}^{m} \binom{m}{j}$ também será par; o que é absurdo, pois $\sum_{j=1}^{m} \binom{m}{j} = 2^m - 1$. ∎

Prova do Teorema 1: ($\Rightarrow$) Suponha $RI(f) = \emptyset$. Temos pelas relações de Girard (ver, *e.g.*, Iezzi, 2001) que $S_j = (-1)^j \; a_{n-j}, \; j = 1, \ldots, n$, onde $S_1 = \sum_{i=1}^{n} x_i$, $S_2 = \sum_{1 \leq i < j \leq n} x_i x_j$, $S_3 = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k, \cdots$, $S_n = x_1 x_2 \cdots x_n$. Com isso, todos os coeficientes $a_j, \; j = 0, \ldots, n-1$, serão pares, e portanto $CI(f) = \emptyset$.

($\Leftarrow$) Pelas relações de Girard, temos que cada $a_j, \; j = 0, 1, \ldots, n-1$, é uma soma de $\binom{n}{n-j}$ termos, sendo cada termo um produto de $n - j$ raízes.

Além disso, se $|RP(f)| = k, \; 0 < k \leq n$, então $\{0, \ldots, k-1\} \subseteq CP(f)$. De fato, cada $a_j, \; j = 0, 1, \ldots, k-1$, terá pelo menos $k - j$ raízes pares como fatores de cada um de seus termos. Ou seja, todos os coeficientes $a_j, \; j = 0, 1, \ldots, k-1$, serão pares.

Agora, para cada coeficiente $a_j, \; j = k, \ldots, n-1$, iremos *ignorar* os termos de sua soma que possuem alguma raiz par, pois os mesmos *não influenciam* na paridade de a_j. Podemos então considerar cada soma (relativa à a_j), como tendo *apenas* $\binom{n-k}{n-j}$ termos, *todos ímpares.*

Temos que se o número de termos ímpares da soma relativa à a_j for ímpar, então a_j será ímpar. Pelo Lema 1, o número de somas contendo um número ímpar de termos (*todos ímpares*) será um número ímpar. Portanto, concluímos que $|\{k \leq j \leq n-1 \ / a_j \text{ é ímpar}\}|$ é um número ímpar, e daí $|CI(f)|$ será ímpar. ■

3 Provas dos Teoremas 2 e 3

Para demonstrarmos os Teoremas 2 e 3, usaremos dois lemas, que por sua vez são conseqüências de um resultado muito interessante sobre divisibilidade de coeficientes binomiais por um número primo arbitrário. Deixaremos sua demonstração para o leitor interessado, pois esse resultado é dado como um exercício no excelente livro Graham (Graham et al., 1995 – Exercício 5.36, p.179).

Critério de divisibilidade para coeficientes binomiais. *Sejam p um número primo e $n \geq m$ inteiros não-negativos tais que*

$$\begin{cases} n &= b_0 + b_1 p + \cdots + b_s p^s \\ m &= c_0 + c_1 p + \cdots + c_s p^s \end{cases},$$

onde $0 \leq b_i, c_i \leq p-1$ são inteiros não-negativos. Então,

$$p \nmid \binom{n}{m} \Leftrightarrow c_i \leq b_i, \ i = 0, 1, \ldots, s.$$

Observações.
(1) A notação $a \nmid b$ significa "a não divide b".

(2) $n \geq m \Rightarrow b_s \geq c_s$. De fato, se $s = 0$ o resultado é trivial. Logo, suponhamos $s > 0$ e $n \geq m$, com $b_s < c_s$. Agora, consideremos o *maior valor possível* para n, a saber, quando $b_0 = b_1 = \cdots = b_{s-1} = p-1$ e $b_s < p-1$. Logo, $n = (b_s+1)p^s - 1$. Por outro lado, consideremos o *menor valor possível* para m, a saber, quando $c_0 = c_1 = \cdots = c_{s-1} = 0$ e $c_s = b_s + 1$. Nesse caso, $m = (b_s+1)p^s = n+1$, o que é uma contradição. ■

Esse Critério de Divisibilidade é uma conseqüência de um teorema de A. M. Legendre (1752-1833), o qual diz que a maior potência de um primo p que divide $n!$, denotada por $E_p(n!)$, é dada por

$$E_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \ldots + \lfloor n/p^s \rfloor, \text{ onde } \lfloor n/p^{s+1} \rfloor = 0.$$

Observação. Para $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, escrevemos $\lfloor a/b \rfloor = q$, onde $a = qb + r$, com $0 \leq r < b$.

Como um corolário quase imediato desse resultado, obtém-se que

$$E_p(n!) = (n - \sum_{i=0}^{s} a_i)/(p-1),$$

onde $n = a_s p^s + \ldots + a_1 p + a_0$, com $0 < a_s < p$ e $0 \leq a_i < p, 0 \leq i < s$.

Por sua vez, a partir desse resultado, chega-se facilmente ao Critério de Divisibilidade. Como um outro corolário, pode-se mostrar (ver Griffin, 1954) que o produto de quaisquer n inteiros positivos consecutivos é divisível por $n!$.

Agora, para demonstrarmos o Teorema 2, faremos uso do seguinte lema:

Lema 2. *Sejam p um número primo e $m \in \mathbb{Z}_+$. Então,*

$$p \nmid \left(\begin{array}{c} m \\ j \end{array} \right),\ j = 0, \ldots, m \Leftrightarrow m = tp^r - 1,\ \textit{onde}\ r, t \in \mathbb{Z}_+,\ 1 \leq t \leq p.$$

Prova: Para cada $0 \leq j \leq m$, escrevamos m e j na base p. Ou seja,

$$\left\{ \begin{array}{rcl} m & = & b_0 + b_1 p + \cdots + b_s p^s \\ j & = & c_0 + c_1 p + \cdots + c_s p^s \end{array} \right.$$

Observemos primeiramente que se $m < p$, então $s = 0$. Também, como $p \nmid m$, teremos $p \nmid m!$, e conseqüentemente $p \nmid \left(\begin{array}{c} m \\ j \end{array} \right),\ j = 0, \ldots, m$. Além disso, podemos escrever $m = (m+1)p^0 - 1$.

Portanto, vamos supor daqui em diante que $m \geq p$.

($\Rightarrow$) Suponhamos que $b_k < p-1$ para algum $0 \leq k \leq s-1$ e considere $j = (p-1)p^k$. Daí, $c_k = p - 1 > b_k$ e, pelo critério de divisibilidade, teremos $p \mid \left(\begin{array}{c} m \\ j \end{array} \right)$. Logo, é necessário que $b_i = p - 1,\ i = 0, \ldots, s-1$. Com isso, obtemos $m = (b_s + 1)p^s - 1$.

($\Leftarrow$) Seja $m = tp^r - 1$, onde $r, t \in \mathbb{Z}_+,\ 1 \leq t \leq p$.

(i) Se $r < s$, então $m \leq p^s - 1$, o que é absurdo.
(ii) Se $r > s + 1$, então $m \geq p^{s+2} - 1 = (p-1)(1 + p + \cdots + p^{s+1})$, o que também é absurdo.
(iii) Se $r = s + 1$, então necessariamente $t = 1$. Nesse caso, teremos $b_i = p - 1,\ i = 0, \ldots, s$ e podemos escrever $m = (p)p^s - 1$.

(iv) Se $r = s$, então necessariamente $t = b_s + 1$, o que corresponde a $b_i = p-1,\ i = 0, \ldots, s-1$.

Portanto, concluímos que $m = (b_s + 1)p^s - 1$. Com isso, $b_i = p-1,\ i = 0, \ldots, s-1$, e assim $b_i \geq c_i,\ i = 0, 1, \ldots, s$. Logo, pelo critério de divisibilidade, teremos $p \nmid \left(\begin{array}{c} m \\ j \end{array} \right),\ j = 0, 1, \ldots, m$. ■

Prova do Teorema 2: ($\Leftarrow$) Já mostramos na parte ($\Leftarrow$) da demonstração do Teorema 1 que se $|RP(f)| = k,\ 0 < k \leq n$, então $\{0, \ldots, k-1\} \subseteq CP(f)$. Agora, aplicando o Lema 2 para $p = 2$ e $m = n - k = 2^t - 1$, concluímos que os coeficientes $a_i,\ i = k, \ldots, n-1$ serão todos ímpares.

($\Rightarrow$) Se $|RI(f)| = 2^t - 1$ e $|RP(f)| = l \neq k$, então, raciocinando como acima, concluímos que $CP(f) = \{0, \ldots, l-1\}$.

Se $|RP(f)| = l \geq k$ e $|RI(f)| \neq 2^t - 1$, então $\{0, \ldots, l-1\} \subsetneq CP(f)$. Ou seja, teremos seguramente que $|CP(f)| > k$.

Considere finalmente o caso $|RP(f)| = l < k$ e $|RI(f)| \neq 2^t - 1$. Na soma correspondente ao coeficiente a_l haverá *exatamente* um termo ímpar (aquele cujos fatores são as $n - l$ raízes raízes ímpares). Portanto, a_l será ímpar. ■

Agora, para demonstrarmos o Teorema 3, usaremos o seguinte lema:

Lema 3. *Sejam p um número primo e $n \in \mathbb{Z}_+$ tal que $n = b_0 + b_1 p + \cdots + b_s p^s$, onde $0 \leq b_i \leq p-1$. Considere o conjunto*

$$Q_p(n) = \left\{ 0 \leq j \leq n \,\middle/\, p \nmid \left(\begin{array}{c} n \\ j \end{array} \right) \right\}.$$

Então, $|Q_p(n)| = \prod_{i=0}^{s} (b_i + 1)$.

Prova: Para cada $0 \leq j \leq n$, podemos escrever $j = c_0 + c_1 p + \cdots + c_s p^s$, onde $0 \leq c_i \leq p-1$. Pelo critério de divisibilidade, a fim de que $p \nmid \left(\begin{array}{c} n \\ j \end{array} \right)$, é necessário e suficiente que $c_i \leq b_i,\ i = 0, \ldots, s$. Como haverá exatamente $b_i + 1$ possibilidades para cada c_i, o lema está provado. ■

Prova do Teorema 3: Observemos que se $RP(f) = \emptyset$, então $Q_2(n) \setminus \{0\} = CI(f)$. Nesse caso, teremos $|CI(f)| = |Q_2(n)| - 1$. Portanto, basta que façamos a representação de n na base 2 e calculemos $|Q_2(n)|$.

Faremos a demonstração dos itens (i) e (ii) e deixaremos o item (iii) como exercício para o leitor.

(i) $n = 2^k(2^j - 1) = (1 + 2 + \cdots + 2^{j-1})2^k$. Logo, $b_i = 0,\ i = 0, \ldots, k-1$ e $b_i = 1,\ i = k, \ldots, k+j-1$. Daí, teremos $|Q_2(n)| = \prod_{i=0}^{j+k-1} (b_i + 1) = 2^j$ e portanto $|CI(f)| = 2^j - 1$. Além disso, como $|CP(f)| = n - |CI(f)|$, teremos $|CP(f)| = (2^k - 1)(2^j - 1)$. Agora, lembremos que se $n = 2^k(2^j - 1)$ for um número perfeito par, então $k = j - 1$ e $2^j - 1$ é primo (ver Simmons, 1987, p.594). Logo, j deverá ser necessariamente primo.

Se $j = 2$, então $|CP(f)| = 3$. Senão, j será ímpar e portanto $k = j - 1 = 2r,\ r \geq 1$. Nesse caso, $|CP(f)| = (2^{2r} - 1)(2^j - 1) = 3(1 + 4 + \cdots + 4^{r-1})(2^j - 1)$, que é divisível por $3|CI(f)|$.

(ii) Se $n = 2^{k+2}(2^{j+1} + 1) - 1$, então podemos escrever $n = 2^{k+2}(2^{j+1} - 1) + (2^{k+3} - 1) = (2^{k+2} + 2^{k+3} + \cdots + 2^{j+k+2}) + (2^{k+3} - 1) = (2^{k+2} - 1) + 2^{j+k+3}$. Logo, $b_i = 1,\ i = 0, \ldots, k+1,\ b_i = 0,\ i = k+2, \ldots, j+k+2$ e $b_{j+k+3} = 1$. Com isso, teremos $|Q_2(n)| = \prod_{i=0}^{j+k+3} (b_i + 1) = 2^{k+3}$ e portanto $|CI(f)| = 2^{k+3} - 1$.

Como uma outra aplicação interessante do critério de divisibilidade para coeficientes binomiais, gostaríamos de enunciar, deixando a demonstração como exercício para o leitor interessado, o seguite resultado:

Proposição. *Sejam p um número primo e $m \geq p$ um natural. Então,*

$$p \mid \left(\begin{array}{c} m \\ j \end{array} \right),\ j = 1, \ldots, m-1 \Leftrightarrow m = p^r,\ \textit{onde } r \in \mathbb{N}.$$

POLEZZI, M.; NÓBREGA NETO, T. P. On the parity of the coefficients from polynomials whose zeros are integral. *Rev. Mat. Estat.,* São Paulo, v.24, n.1, p.53-59, 2006.

▪ *ABSTRACT: Consider a polynomial $f(x) = (x - x_1) \cdots (x - x_n)$, where $x_1, \ldots, x_n \in \mathbb{Z}$. In this paper we shall show three results which relate the number of even/odd coefficients of $f(x)$ with the number of even/odd zeros of $f(x)$. These results are intimately connected to the* Girard's relations *(due to the french-flemish mathematician Albert Girard, 1595-1632) and to a divisibility criterium for binomial coefficients.*

▪ *KEYWORDS: Polynomials whose zeros and coefficients are integral; Girard's relations; divisibility criterium for binomial coefficients.*

Referências

GRAHAM, D. E.; KNUTH, D. E.; PATASHNIK, O. *Matemática concreta*: fundamentos para a ciência da computação. 2. ed. São Paulo: LTC, 1995. 475p.

GRIFFIN, H. *Elementary theory of tumbers*. New York: McGraw Hill, 1954. 198p.

IEZZI, G. *Fundamentos de matemática elementar*. 6. ed. São Paulo: Atual, 2001. v.6. 241p.

SIMMONS, G. F. *Cálculo com geometria analítica*. São Paulo: McGraw-Hill, 1987. v.1. 829p.

Recebido em 09.09.2005.

Aprovado após revisão em 06.02.2006.