Algoritmo de Euclides para o cálculo de r-1 de r Mod D

r n = 1 ; n par

Sugestão: geralmente os índices colocados nos extremos do somatório aparecem no termo que será multiplicado. Há algum tempo atrás – se não me falha a memória, quando lidamos com recorrências – o senhor me enviou um pequeno material sobre somatórios e produtórios: <http://www.cs.yale.edu/homes/aspnes/pinewiki/attachments/SummationNotation/summation-notation.pdf>. Pode-se verificar logo no início do material a definição de somatórios, a partir da qual podemos definir produtórios:

Note que o termo multiplicado tem dependência de i. Proponho o seguinte:

Seja uma função, onde e , onde

Colocando a expressão dessa maneira, deixamos clara a relação agrupamento-termo-elemento e eliminamos a não dependência no produtório. Podemos escrever, para fins práticos, que:

Nada mais é do que os termos dos agrupamentos cujos índices são alternados entre par e ímpar, varrendo todas as combinações para cada valor de (Definido logo abaixo).

Uma maneira menos poluída de escrever:

Onde a expressão:

Nada mais é do que os termos dos agrupamentos cujos índices são alternados entre par e ímpar, varrendo todas as combinações para cada valor de

𝜸 = número de elementos ais por produtório . Cada produtório é um termo do somatório. 𝜸 varia de 1 para j = 0, até n+1 para j = n/2

Sugestão: ao invés de escrever , que dá a ideia do produto de gama, escrever:

Mostrando que é uma variável que depende de e (pois também depende de e ). Colocando a notação dessa maneira, parece-me que eliminamos a ambiguidade variável-produtório e ainda deixamos claro o que a variável significa.

b k : k-ésima linha do triângulo gama

m =

i : índice dos elementos a que compõe cada termo. Esses índices são alternados par-ímpar, varrendo todas as combinações sem permutação, para cada valor de .

Ex: n = 6

; m = 4; : somatório de 4 termos com 1 elemento cada: a0 , a2 , a4 , a6

; m = 3; : somatório de 10 termos com 3 elementos cada: a0.a1.a2 , a0.a1.a4 , a0.a1.a6 , a0.a3.a4 , a0.a3.a6 , a0.a5.a6 , a2.a3.a4 , a2.a3.a6 , a2.a5.a6 , a4.a5.a6

; m = 2; : somatório de 6 termos com 5 elementos cada: a0.a1.a2.a3.a4 , a0.a1.a2.a3.a6 , a0.a1.a2.a5.a6 , a0.a1.a4.a5.a6 , a0.a3.a4.a5.a6 , a2.a3.a4.a5.a6

; m = 1; : somatório de 1 termo com 7 elementos: a0.a1.a2.a3.a4.a5.a6 ;

Portanto,

= = a0 + a2 + a4 + a6 + a0.a1.a2 + a0.a1.a4 , a0.a1.a6 + a0.a3.a4 , a0.a3.a6 + a0.a5.a6 + a2.a3.a4 + a2.a3.a6 + a2.a5.a6 + a4.a5.a6 + a0.a1.a2.a3.a4 + a0.a1.a2.a3.a6 + a0.a1.a2.a5.a6 + a0.a1.a4.a5.a6 + a0.a3.a4.a5.a6 + a2.a3.a4.a5.a6 + a0.a1.a2.a3.a4.a5.a6

E, para n = 6

= = a0 + a2 + a4 + a6 + a0.a1.a2 + a0.a1.a4 , a0.a1.a6 + a0.a3.a4 , a0.a3.a6 + a0.a5.a6 + a2.a3.a4 + a2.a3.a6 + a2.a5.a6 + a4.a5.a6 + a0.a1.a2.a3.a4 + a0.a1.a2.a3.a6 + a0.a1.a2.a5.a6 + a0.a1.a4.a5.a6 + a0.a3.a4.a5.a6 + a2.a3.a4.a5.a6 + a0.a1.a2.a3.a4.a5.a6.

r n = 1 ; n ímpar

Sugestão: seguindo a mesma ideia do caso par, podemos escrever:

Seja uma função, onde e , onde

Uma maneira menos poluída de escrever:

Onde:

Nada mais é do que os termos dos agrupamentos cujos índices são alternados entre par e ímpar, varrendo todas as combinações para cada valor de

𝜸 = número de elementos ais por produtório . Cada produtório é um termo do somatório. 𝜸 varia de 2 para j = 1, até n+1 para j = (n+1)/2

Sugestão: análoga àquela feita no caso par.

b k : k-ésima linha do triângulo gama

m =

i : índice dos elementos a que compõe cada termo. Esses índices são alternados par-ímpar, varrendo todas as combinações sem permutação, para cada valor de .

Ex: n = 5

; m = 3; somatório de 6 termos com 2 elemento cada: a0.a1 , a0.a3 , a0.a5 , a2.a3 , a2.a5 , a4.a5

; m = 2; : somatório de 5 termos com 4 elementos cada: a0.a1.a2.a3 , a0.a1.a2.a5 , a0.a1.a4.a5 , a0.a3.a4.a5 , a2.a3.a4.a5 .

; m = 1; : somatório de 1 termo com 6 elementos : a0.a1.a2.a3.a4.a5 .

Portanto,

= = a0.a1 + a0.a3 + a0.a5 + a2.a3 + a2.a5 + a4.a5 + a0.a1.a2.a3 + a0.a1.a2.a5 + a0.a1.a4.a5 + a0.a3.a4.a5 + a2.a3.a4.a5 + a0.a1.a2.a3.a4.a5 .

E, para n = 5

= = a0.a1 + a0.a3 + a0.a5 + a2.a3 + a2.a5 + a4.a5 + a0.a1.a2.a3 + a0.a1.a2.a5 + a0.a1.a4.a5 + a0.a3.a4.a5 + a2.a3.a4.a5 + a0.a1.a2.a3.a4.a5 .