

# Universidad Nacional de Colombia

## Algebra abstracta y computacional

### Taller 2 Semana 2 - Grupo 9

Paola Andrea Gallegos - 1005257935 - pgallegos@unal.edu.co  
 Oscar Julian Rodriguez - 1022445731- osrodriguezc@unal.edu.co  
 Santiago Diaz Gonzalez - 1007244241 - sdiazgo@unal.edu.co

August 24, 2022

1. Muestre una forma de multiplicar números complejos  $a + bi$  y  $c + di$  usando unicamente tres multiplicaciones de numeros reales. El algoritmo debe arrojar por separado las componentes reales  $ac - bd$  y  $ad + bc$ .

**Desarrollo:** La multiplicación de numeros complejos normalmente implica cuatro multiplicaciones y dos sumas.

$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i.$$

con *Gauss algorithm for complex multiplication* Gauss descubrió una manera de hacer esto con solo tres multiplicaciones, usando esencialmente el mismo cálculo que el algoritmo de Karatsuba:

$$\begin{aligned} k_1 &= c * (a + b) \\ k_2 &= a * (d - c) \\ k_3 &= b * (c + d) \\ \text{Real part} &= k_1 - k_3 \\ \text{Imaginary part} &= k_1 + k_2 \end{aligned}$$

Se puede contar los símbolos  $*$ ,  $+$  y  $-$  de arriba y ver que el primer algoritmo usa 4 multiplicaciones y 2 sumas/restas. El segundo algoritmo utiliza 3 multiplicaciones y 5 sumas/restas.

El algoritmo de Gauss sería más rápido que el algoritmo directo si los componentes fueran números enteros muy grandes o flotantes de muy alta precisión. El tiempo requerido para sumar números enteros de  $n$  dígitos es  $O(n)$ , pero el tiempo requerido para multiplicar números de  $n$  dígitos es al menos  $O(n \log n)$ . Entonces, para  $n$  lo suficientemente grande, vale la pena hacer una suma adicional para ahorrar una multiplicación.

2. Implemente dos funciones *MultEscuela* $[a,b]$  y *Karatsuba* $[a,b]$  en *Mathematica* con los algoritmos de multiplicacion de la escuela y el de Karatsuba, respectivamente. Considere dos enteros.

$$\begin{aligned} a &= \text{Random}[\text{Integer}, \{10, 10^{500}\}] \\ b &= \text{Random}[\text{Integer}, \{10, 10^{500}\}] \end{aligned}$$

Multipliquelos con las dos funciones y con la multiplicacion que ya esta implementada en *Mathematica*. Compare los tiempos de ejecucion. Repita esto con los siguientes enteros:

$$\begin{aligned} a &= \text{Random}[\text{Integer}, \{10^{99}, 10^{100}\}] \\ b &= \text{Random}[\text{Integer}, \{10^{00}, 10^{100}\}] \end{aligned}$$

**Desarrollo:** Primero creamos las dos funciones que vamos a utilizar menos la multiplicación que ya esta implementada en Mathematica

```

In[1]:= $RecursionLimit = ∞;
        [límite de recursión]

Clear[Karatsuba] (*Limpiamos cualquier funcion con este nombre que haya sido creada antes *)
        [borra]

Karatsuba[x_, y_] :=
  (Karatsuba[x, y] = Module[{a, b, c, d, n, m, aporc, bpord},
    [módulo]

    n = Length[IntegerDigits[x]];
    [longitud] [dígitos de entero]

    m = Length[IntegerDigits[x]];
    [longitud] [dígitos de entero]

    m = Max[n, m];
    [máximo]

    n = 1;
    While[n < m, n = 2 * n];
    [mientras]

    b = Mod[x, 10 ^ (n / 2)];
    [operación módulo]

    a = (x - b) / 10 ^ (n / 2);
    d = Mod[y, 10 ^ (n / 2)];
    [operación módulo]

    c = (y - d) / 10 ^ (n / 2);
    aporc = Karatsuba[a, c];
    bpord = Karatsuba[b, d];
    aporc * 10 ^ n + (aporc + bpord
      + Karatsuba[a - b, d - c]) * 10 ^ (n / 2) + bpord) /;

    Min[Length[IntegerDigits[x]], Length[IntegerDigits[y]] > 1
    [mí... [longitud] [dígitos de entero] [longitud] [dígitos de entero]

Karatsuba[x_, y_] := x * y

In[5]:= Clear[MultiEscuela] (*Limpiamos cualquier funcion con este nombre que haya sido creada antes *)
        [borra]

MultiEscuela[x_, y_] :=
  (MultiEscuela[x, y] =
    Module[{a, b, c, d, n, m},
      [módulo]

      n = Length[IntegerDigits[x]];
      [longitud] [dígitos de entero]

      m = Length[IntegerDigits[x]];
      [longitud] [dígitos de entero]

      m = Max[n, m];
      [máximo]

      n = 1; While[n < m, n = 2 * n];
      [mientras]

      b = Mod[x, 10 ^ (n / 2)];
      [operación módulo]

      a = (x - b) / 10 ^ (n / 2);
      d = Mod[y, 10 ^ (n / 2)];
      [operación módulo]

      c = (y - d) / 10 ^ (n / 2);
      MultiEscuela[a, c] * 10 ^ n +
      (MultiEscuela[a, d] + MultiEscuela[b, c]) *
      10 ^ (n / 2) + MultiEscuela[b, d]) /;

      Min[Length[IntegerDigits[x]], Length[IntegerDigits[y]] > 1
      [mí... [longitud] [dígitos de entero] [longitud] [dígitos de entero]

MultiEscuela[x_, y_] := x * y

```

Definimos los números enteros a usar con Random, primero a1 y b1.

\_\_\_\_\_

```

In[15]:= x2 = Random[Integer, {10^99, 10^100}]
           |aleatorio |entero
           |
y2 = Random[Integer, {10^99, 10^100}]
           |aleatorio |entero

Out[15]= 4 144 282 183 963 007 200 139 920 410 832 675 810 023 481 581 690 213 405 793 256 594 604 815 436 954 910 807 093 671 889 426 827 659

Out[16]= 1 553 493 443 181 948 347 360 683 254 705 783 735 821 636 628 521 290 089 785 529 184 725 550 643 159 248 012 924 162 842 641 314 625

In[17]:= Mult4 = x2 * y2

Out[17]= 6 438 115 199 482 296 734 347 547 296 515 955 743 147 116 684 306 679 943 427 908 010 986 629 362 555 343 158 680 690 459 706 276 356 506 688 329 379 847 444 374 293 270 145 193 \
160 459 206 129 680 912 571 554 029 144 094 292 200 870 296 236 026 454 323 071 212 875

In[18]:= Mult5 = MultEscuela[x2, y2]

Out[18]= 6 438 115 199 482 296 734 347 547 296 515 955 743 147 116 684 306 679 943 427 908 010 986 629 362 555 343 158 680 690 459 706 276 356 506 688 329 379 847 444 374 293 270 145 193 \
160 459 206 129 680 912 571 554 029 144 094 292 200 870 296 236 026 454 323 071 212 875

In[19]:= Mult3 = Karatsuba[x2, y2]

Out[19]= 6 438 115 199 482 296 734 347 547 296 515 955 743 147 116 684 306 679 943 427 908 010 986 629 362 555 343 158 680 690 459 706 276 356 506 688 329 379 847 444 374 293 270 145 193 \
160 459 206 129 680 912 571 554 029 144 094 292 200 870 296 236 026 454 323 071 212 875

```

La función incorporada es considerablemente mejor ya que la aritmética de enteros, como el módulo más importante del álgebra combinacional, está completamente implementada en el lenguaje de programación C y reside en el kernel de Mathematica. Los programas que están escritos en el lenguaje de alto nivel de Mathematica no pueden tener la misma eficiencia que las funciones del kernel, encontramos que en el lenguaje de alto nivel de Mathematica, el algoritmo de Karatsuba ya es más rápido para números enteros de 100 dígitos.

```

In[20]:= Timing[Mult4 = x2 * y2] (*Multiplicacion de mathematica*)
           |cronometra
           |
           Timing[Mult5 = MultEscuela[x2, y2]] (*Multiplicacion de MultEscuela*)
           |cronometra
           |
           Timing[Mult6 = Karatsuba[x2, y2]]
           |cronometra
           |
           (*Multiplicacion de Karatsuba*)

Out[20]= {0.000014,
6 438 115 199 482 296 734 347 547 296 515 955 743 147 116 684 306 679 943 427 908 010 986 629 362 555 343 158 680 690 459 706 276 356 506 688 329 379 847 444 374 293 270 145 193 \
160 459 206 129 680 912 571 554 029 144 094 292 200 870 296 236 026 454 323 071 212 875}

Out[21]= {8. * 10^-6,
6 438 115 199 482 296 734 347 547 296 515 955 743 147 116 684 306 679 943 427 908 010 986 629 362 555 343 158 680 690 459 706 276 356 506 688 329 379 847 444 374 293 270 145 193 \
160 459 206 129 680 912 571 554 029 144 094 292 200 870 296 236 026 454 323 071 212 875}

Out[22]= {5. * 10^-6,
6 438 115 199 482 296 734 347 547 296 515 955 743 147 116 684 306 679 943 427 908 010 986 629 362 555 343 158 680 690 459 706 276 356 506 688 329 379 847 444 374 293 270 145 193 \
160 459 206 129 680 912 571 554 029 144 094 292 200 870 296 236 026 454 323 071 212 875}

```

3. Lea la Sección 4.1.4 de la referencia [2] y realice el Ejercicio 3-c) (a mano!).

### Desarrollo:

Se tienen los polinomios:

$$u(x) = 5x^5 + 4x^4 + 3x^3 + 2x^2 + x + 1$$

$$v(x) = 5x^5 - 4x^4 + 3x^3 - 2x^2 + x - 1$$

Las listas correspondientes a los polinomios  $u(x)$  y  $v(x)$  son:

$$U = [(5, 5), (4, 4), (3, 3), (2, 2), (1, 1), (0, 1)]$$

$$V = [(5, 5), (4, -4), (3, 3), (2, -2), (1, 1), (0, -1)]$$

Ahora se construyen dos listas  $S_k$  correspondientes a los productos de cada término de  $v(x)$  con el polinomio  $u(x)$ :

$$S_1 = [(10, 25), (9, 20), (8, 15), (7, 10), (6, 5), (5, 5)]$$

$$S_2 = [(9, -20), (8, -16), (7, -12), (6, -8), (5, -4), (4, -4)]$$

$$S_3 = [(8, 15), (7, 12), (6, 9), (5, 6), (4, 3), (3, 3)]$$

$$S_4 = [(7, -10), (6, -8), (5, -6), (4, -4), (3, -2), (2, -2)]$$

$$S_5 = [(6, 5), (5, 4), (4, 3), (3, 2), (2, 1), (1, 1)]$$

$$S_6 = [(5, -5), (4, -4), (3, -3), (2, -2), (1, -1), (0, -1)]$$

Ahora se combinan  $S_1$  con  $S_2$ ,  $S_3$  con  $S_4$  y  $S_5$  con  $S_6$ :

$$T_1 = [(10, 25), (9, 0), (8, -1), (7, -2), (6, -3), (5, 1), (4, -4)]$$

$$T_2 = [(8, 15), (7, 2), (6, 1), (5, 0), (4, -1), (3, 1), (2, -2)]$$

$$T_3 = [(6, 5), (5, -1), (4, -1), (3, -1), (2, -1), (1, 0), (0, -1)]$$

Ahora se combinan  $T_1$  con  $T_2$  en  $T_4$  y este se combinará con  $T_3$  en  $W$ :

$$T_4 = [(10, 25), (9, 0), (8, 14), (7, 0), (6, -2), (5, 1), (4, -5), (3, 1), (2, -2)]$$

$$W = [(10, 25), (9, 0), (8, 14), (7, 0), (6, 3), (5, 0), (4, -6), (3, 0), (2, -3), (1, 0), (0, -1)]$$

Finalmente:

$$W(x) = 25x^{10} + 14x^8 + 3x^6 - 6x^4 - 3x^2 - 1$$

4. Sean  $a$  y  $b$  enteros y de tamaño  $n = 3^t$ , es decir que tanto  $a$  como  $b$  se pueden escribir como  $a = A_2X^2 + A_1X + A_0 := a(X)$  y  $b = B_2X^2 + B_1X + B_0 := b(X)$  con  $A_2, A_1, A_0, B_2, B_1, B_0$  listas de  $n/3$  digitos y  $X = \beta^{n/3}$ . El producto  $c = ab$  se puede pensar como un polinomio de grado 4 en la indeterminada  $X$ ,

$$\begin{aligned} c &= ab = (A_2X^2 + A_1X + A_0)(B_2X^2 + B_1X + B_0) \\ &= A_2B_2X^4 + A_2B_1X^3 + A_2B_0X^2 + A_1B_2X^3 + A_1B_1X^2 + A_1B_0X + A_0B_2X^2 + A_0B_1X + A_0B_0 \\ &= A_2B_2X^4 + (A_2B_1 + A_1B_2)X^3 + (A_2B_0 + A_1B_1 + A_0B_2)X^2 + (A_1B_0 + A_0B_1)X + A_0B_0 \\ &= C_4X^4 + C_3X^3 + C_2X^2 + C_1X + C_0 \end{aligned}$$

Los coeficientes  $C_0, \dots, C_4$  se pueden determinar evaluando  $c(X)$  en cinco valores diferentes. Consideremos  $x = 0, 1, -1, 2, \infty$ :

- $c(\infty) = C_4 = a(\infty)b(\infty) = A_2B_2$
- $c(0) = C_0 = a(0)b(0) = A_0B_0$
- $c(-1) = C_4 - C_3 + C_2 - C_1 + C_0 = a(-1)b(-1) = A_2B_2 - A_2B_1 - A_1B_2 + A_2B_0 + A_1B_1 + A_0B_2 - A_1B_0 - A_0B_1 + A_0B_0$

Que puede ser factorizado como  $(B_0 + B_2 - B_1)(A_2 - A_1 + A_0)$ .

- $c(1) = C_4 + C_3 + C_2 + C_1 + C_0 = a(1)b(1) = A_2B_2 + A_2B_1 + A_1B_2 + A_2B_0 + A_1B_1 + A_0B_2 + A_1B_0 + A_0B_1 + A_0B_0$

Que puede ser factorizado como  $(B_0 + B_2 + B_1)(A_2 + A_1 + A_0)$ .

Explicitamente se tiene que  $C_0 = A_0B_0$  y  $C_4 = A_2B_2$ , para encontrar los demas coeficientes del sistema se utilizará Mathematica:

```

Solve[c4 == a2 * b2 && c0 == a0 * b0 && c4 - c3 + c2 - c1 + c0 == (b0 + b2 - b1) (a2 - a1 + a0) &&
[resolve
c4 + c3 + c2 + c1 + c0 == (b0 + b2 + b1) (a2 + a1 + a0) &&
16 c4 + 8 c3 + 4 c2 + 2 c1 + c0 == 16 * a2 * b2 + 8 * a2 * b1 + 8 * a1 * b2 + 4 * a2 * b0 + 4 * a1 * b1 + 4 *
a0 * b2 + 2 * a1 * b0 + 2 * a0 * b1 + a0 * b0, {c1, c2, c3, c4, c0}]

Out[3]= {{c1 -> a1 b0 + a0 b1, c2 -> a2 b0 + a1 b1 + a0 b2, c3 -> a2 b1 + a1 b2, c4 -> a2 b2, c0 -> a0 b0}}

```

De esta manera:

- $C_0 = A_0 B_0$

- $C_1 = A_1 B_0 + A_0 B_1$

Utilizando el truco de Karatsuba se puede reescribir como:

$$A_0 B_0 + A_1 B_1 + (A_0 - A_1)(B_1 - B_0)$$

- $C_2 = A_2 B_0 + A_1 B_1 + A_0 B_2$

Utilizando el truco de Karatsuba se puede reescribir como:  $(A_0 + A_1 + A_2)(B_0 + B_1 + B_2) - A_0 B_0 - A_2 B_2 - (A_1 B_0 + A_0 B_1) - (A_2 B_1 + A_1 B_2)$

- $C_3 = A_2 B_1 + A_1 B_2$

Utilizando el truco de Karatsuba se puede reescribir como:  $A_1 B_1 + A_2 B_2 + (A_1 - A_2)(B_2 - B_1)$

- $C_4 = A_2 B_2$

Por lo tanto el producto de  $a$  por  $b$  se puede escribir como:

$$a \cdot b = A_0 B_0 + (A_0 B_0 + A_1 B_1 + (A_0 - A_1)(B_1 - B_0))X + ((A_0 + A_1 + A_2)(B_0 + B_1 + B_2) - A_0 B_0 - A_2 B_2 - (A_1 B_0 + A_0 B_1) - (A_2 B_1 + A_1 B_2))X^2 + (A_1 B_1 + A_2 B_2 + (A_1 - A_2)(B_2 - B_1))X^3 + (A_2 B_2)C^4$$

De esta manera se tienen 5 productos y 12 sumas-restas.

Sea  $T(n)$  el costo de la complejidad del producto de dos  $n$ -dígitos con  $n = 3^t$ . Teniendo en cuenta que el algoritmo de Karatsuba utilizaba 5 productos y 12 sumas-restas, entonces se obtiene que  $T(n) = 5T(n/2) + Cn$  con  $C$  una constante positiva.

Si  $a = 5$  y  $b = 3$  entonces  $\log_3(5) - \epsilon = 1$  luego  $\epsilon = \log_3(5) - 1 = 0.46497 > 0$ . Por lo tanto por el teorema maestro  $T(n) = O(n^{\log_3(5)}) = O(n^{1.46497})$

5. **(Mathematica)** Un entero  $n$  cumple la propiedad AUV-2 si  $n$  es producto de tres primos impares diferentes y además la ecuación diofántica  $x^2 + y^2 = n$  tiene solución. Por ejemplo, 1087985 cumple esta propiedad, en efecto:

$$1087985 = 5 * 37 * 5881$$

Además,  $x^2 + y^2 = 1087985$  tiene solución, por ejemplo (92, 1039) es una de ellas. Encuentre todos los enteros que satisfacen la propiedad AUV-2 en el intervalo  $[2, 10^4]$

### Desarrollo:

Para determinar los números que satisfacen la propiedad AUV-2, es necesario reducir la lista de posibles números primos que se pueden multiplicar en ternas para generar números entre 2 y 10000. Para esto, se tomará el producto de 3 y 5, (los dos primos impares más pequeños posibles) y se multiplicará con otros números primos hasta encontrar el máximo primo  $p$  tal que  $3 * 5 * p < 10000$ . Además, se guardarán en una lista para ahorrar tiempo de cómputo a la hora de realizar las multiplicaciones entre primos.

```

In[2]:= primos = {3, 5};
       n = NextPrime[5];
           |siguiente primo
       While[15 * n < 10000, AppendTo[primos, n]; n = NextPrime[n]]
           |mientras           |añade al final           |siguiente primo

In[5]:= Print[primos]
           |escribe
{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113,
127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241,
251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383,
389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523,
541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661}

In[6]:= longprimos = Length[primos]
           |longitud

```

El algoritmo consiste en tres bucles anidados, el bucle más externo comienza desde el primer elemento del arreglo, mientras que el segundo y tercero inician desde el segundo y tercer elemento respectivamente, asegurando así que no haya dos primos iguales a la hora de realizar el producto. En el bucle más interno, se realiza el producto de los tres primos en las posiciones  $i, j, k$  del arreglo, a continuación, se evalúa si dicho producto es mayor a  $10^4$ , en caso de serlo, se procede a elegir otros elementos de la lista. Si es menor a  $10^4$ , se verifica si es solución a la ecuación diofántica con el comando "PowersRepresentation", si lo es, se añade a la lista de números que cumple con la propiedad AUV-2.

```

i = 1;
numsaUV2 = {};
(*Bucle para elegir el primer elemento del producto*)While[i ≤ longprimos, j = i + 1;
           |mientras
(*Bucle para elegir el segundo elemento del producto*)While[j ≤ longprimos, k = j + 1;
           |mientras
(*Bucle para elegir el tercer elemento del producto*)
While[k ≤ longprimos, producto = primos[[i]] * primos[[j]] * primos[[k]];
           |mientras
(*Evalúa si el producto es mayor a 10^4*)If[producto > 10000, Break[]];
           |si           |finaliza iteración
(*Evalúa si hay solución para la ecuación diofántica*)r = PowersRepresentations[producto, 2, 2];
           |representaciones en sumas de potencias
(*En caso de haber soluciones, añade el
producto a la lista de números AUV-2*)If[Length[r] > 0, AppendTo[numsaUV2, producto]];
           |si |longitud |añade al final
k = k + 1];
j = j + 1];
i = i + 1];
(*Muestra la lista de números que cumplen con la propiedad AUV-2 entre 2 y 10^4*)
Print[numsaUV2];
           |escribe
{1105, 1885, 2405, 2665, 3445, 3965, 4745, 5785, 6305, 6565, 7085, 7345, 8905, 9685, 2465, 3145, 3485,
4505, 5185, 6205, 7565, 8245, 8585, 9265, 9605, 5365, 5945, 7685, 8845, 7585, 9805, 6409, 8177, 9061}

```