Universidad Nacional de Colombia
Departamento de Matemáticas
Álgebra Abstracta y Computacional
Taller Semana 2 (II-2022)

Prof. José L. Ramírez

Los problemas que aparecen señalados con el símbolo 🕮 deben ser resueltos en Mathematica. No olvide que debe justificar cada una de sus respuestas.

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

2. (🕮) Implemente dos funciones `MultEscuela`$[a,b]$ y `Karatsuba`$[a,b]$ en *Mathematica*® con los algoritmos de multiplicación de la escuela y el de Karatsuba, respectivamente. Considere dos enteros

   ```
   In[1]:= a=Random[Integer, {10, 10^500}];

   In[2]:= b=Random[Integer, {10, 10^500}];
   ```

   Multiplíquelos con las dos funciones y con la multiplicación que ya está implementada en *Mathematica*® . Compare los tiempos de ejecución. Repita esto con los siguientes enteros:

   ```
   In[3]:= a=Random[Integer, {10^99, 10^100}];

   In[4]:= b=Random[Integer, {10^99, 10^100}];
   ```

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

4. La identidad en la que se basa el Algoritmo de Karatsuba se puede obtener y generalizar teniendo en cuenta lo siguiente. Sean a y b enteros en base β y de tamaño $n=2^t$. Es decir que a y b se pueden escribir como $a=A+\tilde{A}X:=a(X)$ y $b=B+\tilde{B}X:=b(x)$ con $A,\tilde{A},B,\tilde{B}$ $n/2$ dígitos y $X=\beta^{n/2}$. El producto $c=ab$ se puede pensar como un polinomio de grado 2 en la indeterminada X,

$$c = ab = C_0 + C_1X + C_2X^2 := c(X),$$

donde $C_0 = AB, C_1 = A\tilde{B} + \tilde{A}B$ y $C_2 = \tilde{A}\tilde{B}$. Los coeficientes C_0, C_1 y C_2 se pueden determinar evaluando $c(X)$ en tres valores diferentes. Consideremos $X = 0, -1, \infty$. Para un polinomio cualquiera $p(x)$, la notación $p(\infty)$ corresponde al coeficiente principal de p. Por lo tanto, tenemos que

$$\begin{aligned}
c(\infty) &= C_2 &&= a(\infty)b(\infty) &&= \tilde{A}\tilde{B},\\
c(0) &= C_0 &&= a(0)b(0) &&= AB,\\
c(-1) &= C_0 - C_1 + C_2 &&= a(-1)b(-1) &&= (A - \tilde{A})(B - \tilde{B}),
\end{aligned}$$

Resolviendo este sistema para C_0, C_1, C_2 se obtienen los coeficientes del algoritmo de Karatsuba, es decir, $C_0 = AB$, $C_2 = \tilde{A}\tilde{B}$ y

$$C_1 = C_0 + C_2 - (A - \tilde{A})(B - \tilde{B}) = AB + \tilde{A}\tilde{B} - (A - \tilde{A})(B - \tilde{B}).$$

Generalice la anterior idea, pero en vez de dividir cada entero a y b en dos listas de igual tamaño, divida las listas en tres partes iguales, por ejemplo $a = A_2X^2 + A_1X + A_0$ donde $X = \beta^{n/3}$. Evalúe en los puntos $X = \infty, 0, 1, -1, -2$ y a partir de esta información describa un algoritmo para multiplicar enteros en base β. Luego demuestre que este algoritmo tiene complejidad $O(n^{1,465})$.

5. (Los números AUV-2) 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

$$1087985 = 5 \cdot 37 \cdot 5881.$$

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 $[2, 10^4]$.

. . . .

[Ref 1] K.O. Geddes, S. R. Czapor, G. Labahn. Algorithms for Computer Algebra. Kluwer Academic Publisher, 1992.

[Ref 2] E. A. Lamagna. Computer Algebra, Concepts and Techniques. CRC Press, 2019.