	Departamento de Matemática da Universidade de Coimbra		
	Análise de Algoritmos	**Micro-trabalho 1**	**de 22/02 a 01/03 de 2010**

Suponha que vai multiplicar dois números, x e y, escritos em binário usando n digítos cada (s.p.d.g., vamos supôr que n é uma potência de 2). Vamos particionar cada um em metade:

$$x = 2^{\frac{n}{2}} x_e + w_d \qquad y = 2^{\frac{n}{2}} y_e + y_d \, .$$

Cada x_e, x_d, y_e e y_d tem $n/2$ digitos binários, respectivamente os primeiros $n/2$ na parte esquerda e os restantes na parte direita.

Então,

$$xy = 2^n x_e \, y_e + 2^{\frac{n}{2}} (x_e \, y_d + x_d \, y_e) + x_d \, y_d$$

e

- As multiplicações por potências de 2^k correspondem a "deslocamentos à esquerda" por preenchimento das k posições à direita com o valor binário 0
- As somas são efectuadas em quantidade de operações linear no número de digítos;
- As multiplicações $x_i \, y_j$ são as operações mais pesadas.

Um algoritmo possível para multiplicar x e y seria o seguinte (note-se que $n - m = p - k$):

Multiplica($x[m \,..\, n]$, $y[k \,..\, p]$):

- Se $n - m > 1$:
  1. Multiplica($x[m \,..\, \frac{n}{2}]$, y$[k \,..\, \frac{p}{2}]$);
  2. Multiplica($x[\frac{n}{2} \,..\, n]$, y$[\frac{k}{2} \,..\, p]$);
  3. Multiplica($x[m \,..\, \frac{n}{2}]$, y$[\frac{k}{2} \,..\, p]$);
  4. Multiplica($x[\frac{n}{2} \,..\, n]$, y$[k \,..\, \frac{p}{2}]$);
  5. Calcular: $2^{n-m+1} * (1) + 2^{\frac{n-m+1}{2}} * [(2) + (3)] + (4)$;
- Senão devolve $x[m] \, y[k]$

(a) Calcule o número de operações básicas que este algoritmo efectua para multiplicar os 2 números.

(b) Calcule o número de operações básicas que o algoritmo elementar da multiplicação(relembre a escola primária) efectua para multiplicar os 2 números.

(c) Carl Friedrich Gauss (1777-1855) notou que, apesar do produto de 2 complexos,

$$(a + b\, i)(c + d\, i) = ac - bd + (ad + bc)\, i$$

parecer envolver 4 multiplicações de reais, pode ser efectuado usando apenas 3 multiplicações pois,

$$(ad + bc) = (a + b)(c + d) - ac - bd \, .$$

Se usar a estratégia de Gauss, qual a alteração no número final de operações efectuadas?