## Questão 1 a ser resolvida do capitulo 4

A questão consiste em projetar um multiplicador de 36 bits em RNS que seja mais eficiente que em binário.

a) Determine se os seguintes conjuntos de módulos são co-primos:

1. M1={m1,m2,m3,m4,m5,m6,m7,m8,m9,m10,m11}={2,3,5,7,11,13,17,19,23,29,31};
2. M2={m1,m2,m3,m4,m5}={512,511,255,127,31};
3. M3= {m1,m2,m3,m4,m5,m6,m7}={128,127,129, 65, 31, 17, 7};
4. M4= {m1,m2,m3}={$2^{12}$,$2^{12}$-1,$2^{12}$+1};
5. M5= {m1,m2,m3,m4,m5,m6,m7}={512,127,113,43,29,5,3};
6. M6={m1,m2,m3,m4,m5}={128,127,129,63,65}.

Elimine os que não são co-primos para o seguinte apartado.

b) Indique a faixa dinâmica da estrutura RNS e compare com a eficiência da representação com 36-bits em binário. Elimine para o seguinte apartado os que não atingem os 36 bits de representação na saída. Justifique.

c) As tabelas seguintes mostram os resultados de síntese em ASIC para uma tecnologia de UMC do atraso de multiplicadores RNS e de unidades binário-RNS e RNS-binário para os módulos apresentados no apartado a). Tendo em consideração que uma multiplicação em binário de 36 bits é 4.4ns, escolha o conjunto de módulos (apenas existe um conjunto possível) que permite uma operação de multiplicação (e conversões Bin-RNS e RNS-Bin) de forma mais veloz que em binário. Justifique.

**Atraso unidades conversão RNS**

| Conjunto | Bin-RNS | RNS-Bin |
|---|---|---|
| M1 | 1ns | 2.5ns |
| M2 | 1.4ns | 2.4ns |
| M3 | 1.4ns | 2.6ns |
| M4 | 2ns | 1.5ns |
| M5 | 1.5ns | 1.3ns |
| M6 | 1.4 | 2ns |

**Atraso unidades multiplicação RNS**

| Modulo | Multiplier | Modulo | Multiplier | Modulo | Multiplier | Modulo | Multiplier |
|---|---|---|---|---|---|---|---|
| 2 | 0.5ns | 17 | 1.1ns | 63 | 1.1ns | 255 | 1.3ns |
| 3 | 0.6ns | 19 | 1.3ns | 65 | 1.3ns | 511 | 1.4ns |
| 5 | 0.8ns | 23 | 1.4ns | 113 | 1.5ns | 512 | 1ns |
| 7 | 0.6ns | 29 | 1.4ns | 127 | 1.2ns | $2^{12}$-1 | 1.7ns |
| 11 | 1ns | 31 | 1ns | 128 | 0.8ns | $2^{12}$ | 1.2ns |
| 13 | 1ns | 43 | 1.5ns | 129 | 1.4ns | $2^{12}$+1 | 2ns |

d) Aplicando o algoritmo novo CRT-I para o conjunto obtido, a operação modular, M/m1, (onde M é o produtorio de todos os módulos) fica simples ou complexa? (não é preciso resolver a equação apenas obter qual seria a operação modular). Justifique.