a)

1. todos os números são primos, portanto são co-primos

2.

nº	512	511	255	127	31
divisores	256	73	85	1	1
	128	7	51		
	64	1	17		
	32		15		
	16		5		
	8		3		
	4		1		
	2				
	1				

nenhum divisor além de 1 em comum, são co-primos

3

nº	128	127	129	65	31	17	7
divisores	64	1	43	13	1	1	1
	32		3	5			
	16		1	1			
	8						
	4						
	2						
	1						

nenhum divisor além de 1 em comum, são co-primos

4

nº	2^{12}	$2^{12}-1$		$2^{12}+1$
divisores	2^{11}	1365	45	241
	2^{10}	819	39	17
	2^9	585	35	1
	⋮	455	21	
	2^1	315	15	
	2^0	273	13	
		195	9	
		117	7	
		105	5	
		91	3	
		65	1	
		63		

nenhum divisor além de 1 em comum, são co-primos

5.

nº	512	127	113	43	29	5	3
divisores	256	1	1	1	1	1	1
	128						
	64						
	32						
	16						
	8						
	4						
	2						
	1						

nenhum divisor além de 1 em comum, são co-primos

6.

nº	128	127	129	63	65
divisores	64	1	43	9	13
	32		7	7	5
	16		1	3	1
	8			1	
	4				
	2				
	1				

MDC (129, 63) = 7 ≠ 1, conjunto não possui apenas co-primos

b)

$DR(M1) = 200560490130 > 2^{36} - 1$

$DR(M2) = 262661521920 > 2^{36} - 1$

$DR(M3) = 502834899840 > 2^{36} - 1$

$DR(M4) = 687194726240 < 2^{36} - 1$ descartado

$DR(M5) = 1374389052960 > 2^{36} - 1$

para identificar qual conjunto cobre a faixa $[0, 2^{36}-1]$ e é tem DR mais próximo de $2^{36}-1$ realizamos as operações abaixo

$DR(M1) - 2^{36}-1 = 131\,841\,013\,395$

$DR(M2) - 2^{36}-1 = 193\,942\,045\,185$

$DR(M3) - 2^{36}-1 = 434\,115\,423\,105$

$DR(M5) - 2^{36}-1 = 687\,194\,762\,25$ → menor

portanto M5 é o conjunto de módulos mais eficiente

c)

tempo em binário = 4.4 ns

tempo em RNS :

$t(BIN \to RNS) + t(\text{mult } m_i) + t(RNS \to BIN)$

↳ maior $t(\text{mult } m_i)$ $i = 1, 2, \ldots n$

M1 = 1 + 1.4 + 2.5 = 4.9ns
M2 = 1.4 + 1.4 + 2.4 = 5.2ns
M3 = 1.4 + 1.4 + 2.6 = 5.4ns
M5 = 1.5 + 1.5 + 1.3 = 4.3ns → mais eficiente

d) $M5 = \{512, 127, 113, 43, 29, 5, 3\}$

$$\frac{M}{m_1} = \frac{512 \cdot 127 \cdot 113 \cdot 43 \cdot 29 \cdot 5 \cdot 3}{512} = 2^{28} - 1$$

portanto a operação modular é simples