① $\gcd(a, m)$ is a common divisor of a & m.

Since $a \equiv b \bmod m$ $\exists k$ $b = a + km$

$\therefore \gcd(a,m) \mid b$ so $\gcd(a,m)$ is a common divisor of b and m.

$\therefore \gcd(a,m) \mid \gcd(b,m)$

Similarly $\gcd(b,m) \mid \gcd(a,m)$

$\therefore \gcd(a,m) = \gcd(b,m)$ ☺

Alt: Can show integer combinations of a, m are the same as integer comb. of b and m.

Eg. $sb + tm = s(a + km) + tm$
$= sa + (sk + t)m$

If we take all those > 0, then we have the same min (gcd). ☺

The converse does not hold, for example

Let $m = 3$, $a = 2$, $b = 10$. Then

$\gcd(a,m) = 1 = \gcd(b,m)$

But $a \not\equiv b \bmod m$ $a - b = -8$ is not div. by 3 ☹

(2) $244 = 224 + 20$ $\quad$ $20 = 244 - 224$

$224 = 11 \cdot 20 + 4$ $\quad$ $4 = 224 - 11 \cdot 20$

$20 = 5 \cdot 4$

gcd.

$$4 = 224 - 11 \cdot 20 = 224 - 11(244 - 224)$$

$$= -11 \cdot 244 + 12 \cdot 224$$

Bézout coeffs.

(3) $x \equiv 1 \bmod 7$ $\quad$ $x \equiv 2 \bmod 8$ $\quad$ $x \equiv 3 \bmod 9$

Note: 7, 8, 9 – pairwise co-prime. ☺

$m = 7 \cdot 8 \cdot 9 = 504$

m_i	$M_i = \frac{m}{m_i}$	M_i^{-1}	b_i	$M_i M_i^{-1} b_i$
7	$72 \to 2$	4	1	288
8	$63 \to 7 = (-1)$	7	2	882
9	$56 \to 2$	5	3	840
			+	2010

$$\boxed{x \equiv 498 \bmod 504}$$

(4) $2^n \geq n+1$

n	2^n	$n+1$	
0	1	1	✓
1	2	2	✓
2	4	3	✓ ← Basis

By induction

Let $n \geq 1$ $\qquad 2^n = 2 \cdot 2^{n-1} \geq 2\left[(n-1)+1\right] =$

$= 2n = n + n \geq n+1$ ☺