HW11 Sol'ns

1) $2^{105723} \equiv 2^k \mod 13$ if $105723 \equiv k \mod \phi(13)$

$\phi(13) = 12 \qquad 105723 = 12 \cdot 8810 + 3$

$\Rightarrow 2^{105723} \equiv 2^3 \equiv 8 \mod 13$

2) No, consider $n=5$, $a=4$, so $a \perp n$ and $\phi(n) = 4$,

but $4^2 \equiv 16 \equiv 1 \mod 5$.

3) Let $f: S_{ab} \to S_a \times S_b$

$f(x) = (r, s)$ $\quad r$ = remainder of $x \mod a$

s = remainder of $x \mod b$.

Claim: $x \perp ab \iff r \perp a$ and $s \perp b$.

$x = r + ka$
$x = s + \ell b$ by defn of remainder, so $\gcd(x,a) = \gcd(r,a)$
$\gcd(x,b) = \gcd(s,b)$.

Thus, $x \perp ab \Rightarrow x \perp a$ and $x \perp b \Rightarrow r \perp a$ and $s \perp b$

and $r \perp a$ and $s \perp b \Rightarrow x \perp a$ and $x \perp b$ which, with a, b coprime implies $x \perp ab$.

In particular, this means f is well-defined, since $x \in S_{ab} \Rightarrow (r, s) \in S_a \times S_b$.

Now, since (a, b) coprime, by CRT, $\forall (r, s) \in \mathbb{Z}^2$, there is a unique $z \in \{0, \dots, ab-1\}$

s.t. $z \equiv r \mod a$
$z \equiv s \mod b$.

For $(r, s) \in S_a \times S_b$, our claim implies $z \in S_{ab}$. Thus there is an inverse function, so $f : S_{ab} \to S_a \times S_b$ is a bijection, and

$$\phi(ab) = |S_{ab}| = |S_a \times S_b| = |S_a| \times |S_b| = \phi(a)\phi(b).$$

---

4) Note that $x \equiv y \mod n$, $x \equiv y \mod m$ implies $n \mid (x-y)$ and $m \mid (x-y)$. Since n and m are coprime, this implies $n \cdot m \mid (x-y)$, so $x \equiv y \mod nm$

---

5) $n_1 = 11$
$n_2 = 17$
$n_3 = 18$

$N = 3{,}366$

$m_1 = 306$
$m_2 = 198$
$m_3 = 187$

$m_1 \equiv 9 \mod 11$
$m_2 \equiv 11 \mod 17$
$m_3 \equiv 7 \mod 18$

$y_1 = 5$
$y_2 = -3$
$y_3 = -5$

$x \equiv 4y_1m_1 + 3y_2m_2 + 6y_3m_3 \mod 3366$
$\equiv 13770 - 1782 - 5610 \mod 3366$
$\equiv 6378 \equiv 3012 \equiv -354 \mod 3366$