4.2.03 If $a \equiv b \pmod{n}$ prove that $\gcd(a, n) = \gcd(b, n)$.

Proof. Let $a \equiv b \pmod{n}$ then $n|a-b \Rightarrow a-b = nk$ for some $k \in \mathbb{Z}$. Let $d = \gcd(a, n)$ and $e = \gcd(b, n)$. Then, $d|a$ and $d|n \Rightarrow d|(a - nk) \Rightarrow d|b$. Using this fact, as $d|n$ and $d|b \Rightarrow d|\gcd(b, n) \Rightarrow d|e$
Going the other direction, $e|b$ and $e|n \Rightarrow e|(b + nk) \Rightarrow e|a$.
Thus, $e|n$ and $e|a \Rightarrow g|\gcd(a, n) \Rightarrow e|d$
Therefore, as $e|d$ and $d|e$, we have $\gcd(a, n) = \gcd(b, n)$ □

4.2.6c For $n \geq$, use congruence theory to establish each of the following divisibility statement: $27|2^{5n+1} + 5^{n+2}$

Proof. Notice that $32 \equiv 5(\bmod 27)$. Thus, $2^5 \equiv \pmod{27}$
Then, we have $2^{5n} \equiv 5^n \pmod{27}$. Then $2^{5n} \cdot 2 \equiv 2 \cdot 5^n (\bmod 27)$
Observe.

$$\begin{aligned} 2^{5n+1} + 5^{n+2} &\equiv 2 \cdot 5^n + 5^{n+2} \pmod{27} \\ &\equiv 5^n(2 + 25) \pmod{27} \\ &\equiv 5^n \cdot 27 \pmod{27} \\ &\equiv 0 \pmod{27} \end{aligned}$$

Therefore, $27|2^{5n+1} + 5^{n+2}$ □

4.2.8d Prove if the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

Proof. Let $a \in \mathbb{Z}$ such that a is not divisible by 2 or 3. As a is not divisible by 2, then a is odd. Notice. For some $k \in \mathbb{Z}$.

$$a^2 = (2k + 1)^2 = 2k^2 + 4k + 1 = 4k(k + 1) + 1$$

By looking at the parity, we know that $2|K(k + 1) \Rightarrow k(k + 1) = 2l$ for some $l \in \mathbb{Z}$.
Thus, $4(2l) + 1 = 8l + 1$.
Thus, $a^2 \equiv 1 \pmod{8}$. Then, $8|a^2 - 1$. As a is not divisible by 3, then for some $q \in \mathbb{Z}, a = 3q + 1$ or $a = 3q + 2$

Case $a = 3q + 1$ $a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$
So, $a^2 - 1 = 3(3q^2 + 2q) \Rightarrow 3|a^2 - 1$

Case $a = 3q + 2$ $a^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$
So, $a^2 - 1 = 3(3q^2 + 4q + 1) + 1 \Rightarrow 3|a^2 - 1$

Thus, in both cases $3|a^2 - 1$
Therefore, as $8|a^2 - 1$, $3|a^2 - a$, and $\gcd(3, 8) = 1$, then $24|a^2 - 1 \Rightarrow a^2 \equiv (\bmod 24)$ □

4.2.16 Use the theory of congruences to verify that $89|2^{44}-1$ and $97|2^{48}-1$.

$$\begin{aligned}2^{44}-1 &\equiv (2^{11})^4 - 1 \pmod{89}\\ &\equiv (1)^4 - 1 \pmod{89}\\ &\equiv 1-1 \pmod{89}\\ &\equiv 0 \pmod{89}\end{aligned}$$

Thus, $89|2^{44}-1$

$$\begin{aligned}2^{48}-1 = (2^6)^8 - 1 &\equiv 64^8 - 1 \pmod{97}\\ 64^8 = (64^2)^4 &\equiv 1^4 - 1 \pmod{97}\\ &\equiv 1-1 \pmod{97}\\ &\equiv 0 \pmod{97}\end{aligned}$$

Thus, $97|2^{48}-1$

4.2.18 If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod{n}$ where the integer $n = \gcd(n_1, n_2)$.

Proof. Let $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$.
So $n_1|a-b \Rightarrow a-b = n_1k_1, k_1 \in \mathbb{Z}$
and $n_2|a-c \Rightarrow a-c = n_2k_2, k_2 \in \mathbb{Z}$
Thus, $b-c = n_2k_2 - n_1k_1$.
Let $n = \gcd(n_1, n_2) \Rightarrow n|n_1$ and $n|n_2$.
So $n|(n_2k_2 - n_1k_1) \Rightarrow n|b-c$
Thus, $b \equiv c \pmod{n}$ where $n = \gcd(n_1, n_2)$ $\square$