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

Proof. Suppose that $a \equiv b \pmod{n}$. Let $d = \gcd(a, n)$ and $e = \gcd(b, n)$. Then $nk = a - b$ for some $n \in \mathbb{Z}$. Note that $d \mid a$ and $d \mid n$ implies that $a = ud$ and $n = vd$ for $u, v \in \mathbb{Z}$. Then

$$\begin{aligned} nk &= a - b \\ vdk &= du - b \\ b &= d(u - vk) \end{aligned}$$

implies that $d \mid b$. Since $d \mid b$ and $d \mid n$ we see that $d \mid e$. So $d \leq e$. Similarly, $e \mid b$ and $e \mid n$ implies that $b = xe$ and $n = ye$ for some $x, y \in \mathbb{Z}$. Observe that

$$\begin{aligned} nk &= a - b \\ yek &= a - xe \\ a &= e(yk + x) \end{aligned}$$

gives $e \mid a$. Since $e \mid a$ and $e \mid n$, we have $e \mid d$. Therefore $e \leq d$. Thus $e = d$.

□

4.2.6(c) For $n \geq 1$, establish $27 \mid 2^{5n+1} + 5^{n+2}$.

Proof. Let $n \geq 1$. Notice that

$$2^{5n+1} = 2 \cdot 32^n \equiv 2 \cdot 5^n \pmod{27}.$$

Then

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

Thus $27 \mid 2^{5n+1} + 5^{n+2}$. □

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

Proof. Suppose that the integer a is not divisible by 2 or 3. Then $a = 12k + r$ where $r = 1, 5, 7$, or 11.

For $r = 1$: $(12k + 1)^2 = 6 \cdot 24k^2 + 24k + 1 \equiv 1 \pmod{24}$.

For $r = 5$: $(12k + 5)^2 = 6 \cdot 24k^2 + 24 \cdot 5k + 1 \equiv 1 \pmod{24}$.

For $r = 7$: $(12k + 7)^2 = 6 \cdot 24k^2 + 24 \cdot 7k + 1 \equiv 1 \pmod{24}$.

For $r = 11$: $(12k + 11)^2 = 6 \cdot 24k^2 + 24 \cdot 11k + 121 \equiv 1 \pmod{24}$.

Thus $a^2 \equiv 1 \pmod{24}$. □

4.2.16 Use the theory of congruence to verify that

$$89 \mid 2^{44} - 1 \quad \text{and} \quad 97 \mid 2^{48} - 1.$$

Proof. We want to show that 89 divides $2^{44} - 1$. Notice that

$$2^{44} = (2^{11})^4 = (2048)^4 \equiv 1^4 \pmod{89}.$$

So

$$2^{44} - 1 \equiv 1 - 1 \equiv 0 \pmod{89}.$$

Thus $89 \mid 2^{44} - 1$. □

Proof. We want to show that 97 divides $2^{48} - 1$. Notice that

$$2^{48} = (2^{12})^4 = (4096)^4 \equiv 22^4 \pmod{97}.$$

Then

$$22^4 = 484^2 \equiv 96^2 \equiv (-1)^2 \pmod{97}.$$

Therefore

$$2^{48} - 1 \equiv 96^2 - 1 \equiv (-1)^2 - 1 \equiv 0 \pmod{97}.$$

Thus $97 \mid 2^{48} - 1$. □

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. Suppose $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$. Let $n = \gcd(n_1, n_2)$. Then $a - b = kn_1$ for some $k \in \mathbb{Z}$. Since $n \mid n_1$, we see that $n_1 = ln$ for some $l \in \mathbb{Z}$. Therefore $a - b = kln$ implying that $a \equiv b \pmod{n}$. Similarly, since $n \mid n_2$, we find that $n_2 = rn$ for some $r \in \mathbb{Z}$. Then since we know $a - c = xn_2$ for some $x \in \mathbb{Z}$, we see that $a - c = xrn$. Therefore $a \equiv c \pmod{n}$. Thus since $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, it follows that $b \equiv c \pmod{n}$. □