

► **Problem 4.5-21(b)** Find a positive integer x such that $ab \equiv x$ modulo a suitable integer. Assuming that $ab < 50000$, find ab itself, if possible, and explain your reasoning.

$$a \equiv 7, b \equiv 7 \pmod{8}$$

$$a \equiv 9, b \equiv 8 \pmod{27}$$

$$a \equiv 29, b \equiv 18 \pmod{125}$$

Solution.

$$ab \equiv 7 \cdot 7 \equiv 1 \pmod{8}$$

$$ab \equiv 9 \cdot 8 \equiv 18 \pmod{27}$$

$$ab \equiv 29 \cdot 18 \equiv 22 \pmod{125}$$

We first solve $ab \equiv 1 \pmod{8}$ and $ab \equiv 18 \pmod{27}$

Since $1 = 3 \cdot 27 + (-10) \cdot 8$, we obtain

$$ab \equiv 1 \cdot 3 \cdot 27 + 18 \cdot (-10) \cdot 8 = -1359 \equiv 153 \pmod{216}.$$

Then, we solve $ab \equiv 22 \pmod{125}$ and $ab \equiv 153 \pmod{216}$.

Since $1 = (-19) \cdot 125 + 11 \cdot 216$, we obtain

$$ab \equiv 153 \cdot (-19) \cdot 125 + 22 \cdot 11 \cdot 216 = -311103 \equiv 12897 \pmod{27000}.$$

Since $ab < 50000$, we have $x = 12897$ or $x = 39897$. □