

Problem 4.30. Show that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

The converse of Problem 4.30 need not be true. For example, $4 \cdot 7 \equiv 2 \cdot 2 \pmod{12}$. However 7 is not congruent to 2 modulo 12.

Theorem 4.31. Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{3}$ if and only if $2a + b \equiv 0 \pmod{3}$.

Proof. Suppose $a \equiv b \pmod{3}$. Then there exists $k \in \mathbb{Z}$ such that $(a - b) = 3k$ which implies $2(a - b) = 6k$. Moreover, $2a - 2b + 3b = 6k + 3b$ which implies $2a + b = 6k + 3b = 3(2k + b)$. It follows that $2a + b \equiv 0 \pmod{3}$. Conversely, suppose $2a + b \equiv 0 \pmod{3}$. Then there exists $k \in \mathbb{Z}$ such that $2a + b = 3k$. Hence $b = 3k - 2a$. Now

$$a - b = a - (3k - 2a) = 3a - 3k = 3(a - k).$$

Therefore $a \equiv b \pmod{3}$. □

Theorem 4.32. (Fermat's Little Theorem) Let p be a prime and $c \in \mathbb{Z}$. If c is not divisible by p then $c^p \equiv c \pmod{p}$.

Problem 4.33. Determine $5^{17} \pmod{17}$.