

1.18 Theorem. Let $a, b, k, n \in \mathbb{Z}$ with $k, n > 0$. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Proof. Let $a, b, k, n \in \mathbb{Z}$ with $k, n > 0$ be given such that $a \equiv b \pmod{n}$. Consider the base case where $k = 1$. By definition, $a - b = nx$ for some $x \in \mathbb{Z}$, which proves the base case.

By induction, we want to show $a^{t+1} \equiv b^{t+1} \pmod{n}$, provided $a^t \equiv b^t \pmod{n}$ for some $t \in \mathbb{Z}$. By definition, $a - b = nx$ (remembering $a = nx + b$) and $a^t - b^t = ny$ for some $x, y \in \mathbb{Z}$.

$$\begin{aligned}
 a^{t+1} - b^{t+1} &= aa^t - bb^t \\
 &= (nx + b)a^t - bb^t \\
 &= nxa^t + ba^t - bb^t \\
 &= nxa^t + b(a^t - b^t) \\
 &= nxa^t + b(ny) \\
 &= n(xa^t + by).
 \end{aligned}$$

By CPI, $xa^t + by = z$ for some $z \in \mathbb{Z}$. Thus, $a^{t+1} \equiv b^{t+1} \pmod{n}$, and $a^k \equiv b^k \pmod{n}$. \square