Math 302 I.4

Raiden van Bronkhorst

2 March 2020

If a, b, and n are natural numbers with $a \equiv b(\text{mod } n)$, then $a^k \equiv b^k(\text{mod } n)$ for every natural number k.

Proof. Base case. when $k = 0$, the statement is $a^0 \equiv b^0 = 1 \equiv 1(\text{mod } n)$ which is true by Theorem 4.2 (Reflexive property of congruence).

Now suppose $a^k \equiv b^k(\text{mod } n)$ for some natural number $k \geq 0$. Since we know $a \equiv b(\text{mod } n)$, by Theorem 4.6[1] we know $a^k a \equiv b^k b = a^{k+1} \equiv b^{k+1}(\text{mod } n)$. Therefore $a^k \equiv b^k(\text{mod } n)$ for every natural number k. $\square$

[1] If $a \equiv b(\text{mod } n)$ and $c \equiv d(\text{mod } n)$, then $ac \equiv bd(\text{mod } n)$.