Proof of 3.1 12a

Cedric Gerdes

15 February 2021

Definition. Let $n \in \mathbb{N}$. If a and b are integers, then we say that a is congruent to b modulo n provided that n divides $a - b$, which is commonly written as $a \equiv b \pmod{n}$. This implies there exists an integer k such that $a = b + nk$.

Let n be a natural number and let a, b, c, and d be integers. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$.

Proof. By definition, we can rewrite the three statements in the hypothesis as

$$a = b + nk_1$$

$$c = d + nk_2$$

$$a + c = (b + d) + nk_3$$

where k_1, k_2, and k_3 are all, possibly distinct, integers. To prove our desired conclusion we need to show that there exists an integer k_3 which satisfies the third equation. So, substituting the first two equations into the third, we find

$$b + nk_1 + d + nk_2 = (b + d) + nk_3$$

Now using associativity and distributivity

$$(b + d) + n(k_1 + k_2) = (b + d) + nk_3$$

Once this is done it is easy to see that an integer k_3 exists which satisfies this equation, namely $k_1 + k_2$. So, given a is congruent to b and c is congruent to d, then the sum of a and c must be congruent to the sum of b and d. □