In this document, we look at a proof about modular equivalence of a form of arithmetic.

Theorem 1. *If* a*,* b*,* c*, and* d *are integers, and* n *a natural number, such that* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$*, then* $(a + c) \equiv (b + d) \pmod{n}$*.*

Proof. We assume that a, b, c, and d are integers, and n a natural number, such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, and will show that $(a + c) \equiv (b + d) \pmod{n}$. Since $a \equiv b \pmod{n}$ we know that $a - b = kn$ for some integer k and similarly $c - d = mn$ for some integer m. Adding these equations yields

$$\begin{aligned}(a - b) + (c - d) &= kn + mn \\ (a + c) - (b + d) &= (k + m)n\end{aligned}$$

In other words, n divides $(a + c) - (b + d)$, which by the definition of modular congruence means that $(a + c) \equiv (b + d) \pmod{n}$. We have now shown that if a, b, c, and d are integers, and n a natural number, such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$. □