Modular Multiplication is Well-Defined

Katherine Stange, CU Boulder, MATH 2001

Theorem 1. *Let $n \in \mathbb{Z}$. Let $a, b, c, d \in \mathbb{Z}$. Suppose that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then $ab \equiv cd \pmod{n}$.*

Proof. By assumption, $n \mid a - c$ and $n \mid b - d$. Therefore,

$$a - c = nk, \quad b - d = n\ell.$$

In other words,

$$a = c + nk, \quad b = d + n\ell.$$

So,

$$ab = (c + nk)(d + n\ell) = cd + n(kd + n\ell + nk\ell).$$

Therefore, $ab - cd$ is divisible by n and hence $ab \equiv cd \pmod{n}$. □