同餘的運算

假設 $n \in \mathbb{Z}^+$，若 $a \equiv b \pmod{n}$ 且 $c \equiv d \pmod{n}$，則

1. $a + c = b + d \pmod{n}$

2. $ac = bd \pmod{n}$

證明：

因為 $a \equiv b \pmod{n}$，則存在 $s \in \mathbb{Z}$，使得

$a = b + sn$ — ① ；

因為 $c \equiv d \pmod{n}$，則存在 $t \in \mathbb{Z}$，使得

$c = d + tn$ — ②

1. ① + ② $\Rightarrow$ $a + c = b + d + sn + tn = b + d + n(s+t)$

$\Rightarrow$ $a + c \equiv b + d \pmod{n}$ ※

2. ① × ② $\Rightarrow$ $ac = (b+sn)(d+tn) = bd + btn + dsn + stn^2$

$= bd + n(bt + ds + stn)$

$\Rightarrow$ $ac \equiv bd \pmod{n}$ ※