What kinds of operations are we allowed to do to a modular equivalence?

Thm For all $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

if $a \equiv_m b$ and $c \equiv_m d$, then

1. $a + c \equiv_m b + d$

(modular equivalence "plays nice" w/ addition — $\equiv_m$ is a congruence w/ respect to addition)

2. $a - c \equiv_m b - d$
3. $ac \equiv_m bd$

Proof Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ be arbitrary, and suppose $a \equiv_m b$ and $c \equiv_m d$. By a previous theorem, we can write

$a = b + jm$ and $c = d + km$ for some integers j and k.

$(a \equiv_m b) \longleftrightarrow (\exists k.\ a = b + km)$

1. $a + c = (b + jm) + (d + km)$
   $= (b + d) + (jm + km)$
   $= (b + d) + (j + k)m$

   Thus, by the same theorem, $a + c \equiv_m b + d$.

2. $a - c = (b + jm) - (d + km)$
   $= (b - d) + (jm - km)$
   $= (b - d) + (j - k)m$ $\longrightarrow$ $a - c \equiv_m b - d$

3. $ac = (b + jm)(d + km)$
   $= bd + m(\text{stuff})$ $\longrightarrow$ $ac \equiv_m bd$.

   ↓ don't care, everything else will have multiple of m.

Corollary: $(a + b) \bmod m \equiv_m a \bmod m + b \bmod m$

$(ab) \bmod m \equiv_m (a \bmod m)(b \bmod m)$

Ex. $x + 7 \equiv_3 12$.

Note $7 \equiv_3 7$ (since $\equiv_3$ is reflexive) so, by the previous theorem, $x + 7 - 7 \equiv_3 12 - 7$

$\rightarrow x \equiv_3 5$.

Also note that $5 \equiv_3 2$, so, by transitivity,

$\boxed{x \equiv_3 2.}$ — Simplest form — $x \equiv_m k$ where $0 \leq k < m$.

This actually means

$x \in \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

We can check by substituting for x:

- $x = 2$: $2 + 7 \equiv_3 12 \rightarrow 9 \equiv_3 12$ ✓
- $x = 8$: $8 + 7 \equiv_3 12$ ✓

Ex* Solve for x: $101x + 52 \equiv_{10} 68$.

$-52 \quad -52$

$\rightarrow 101x \equiv_{10} 16 \equiv_{10} 6$

Can't divide both sides. But note $101 \equiv_{10} 1$.

And because $\equiv_{10}$ is a congruence for multiplication, and $x \equiv_{10} x$ by reflexivity, therefore $101x \equiv_{10} 1x$.; then by transitivity + symmetry

$x \equiv_{10} 101x \equiv_{10} 6$

So $x \equiv_{10} 6$.

In practice, can just write:

$$101x + 52 \equiv_{10} 68$$

{subtract 52}

$$\rightarrow \quad 101x \equiv_{10} 16$$

{$101 \equiv_{10} 1$, $16 \equiv_{10} 6$}

$$\rightarrow \quad x \equiv_{10} 6$$

Ex $\quad 3x + 19 \equiv_7 2(x - 73)$

$$\rightarrow \quad 3x + 19 \equiv_7 2x - 146$$

$$\rightarrow \quad 3x \equiv_7 2x - 165$$

$$\rightarrow \quad x \equiv_7 -165$$

$$\rightarrow \quad x \equiv_7 \underline{3} \equiv_7 -4$$

Ex $\quad x + 22 \equiv_{19} 20x + 3$

Ex $\quad x + 22 \equiv_{19} 20x - 7$