

Please explain why it follows from  $X \equiv x \pmod{b}$  and  $Y \equiv y \pmod{b}$  that  $X + Y \equiv x + y \pmod{b}$ .

**Proof:**

$X \equiv x \pmod{b}$  means that  $X$  and  $x$  differ by a multiple of  $b$ , or  $X = kb + x$  for some integer  $k$ . Likewise  $Y = mb + y$  for some integer  $m$ . Then

$$X + Y = (kb + x) + (mb + y) = (k + m)b + (x + y).$$

That is,  $X+Y$  and  $x + y$  differ by a multiple of  $b$ , so  $X + Y \equiv x + y \pmod{b}$ .