

Prop 1.20

$$(-m)(-n) = -((-m) \cdot n)$$

$$\stackrel{\text{case x}}{=} - (n \cdot (-m))$$

$$\stackrel{\text{cl. 1}}{=} -(- (n \cdot m))$$

--x: negated color

$$= nm$$

$$\stackrel{\text{comm.}}{=} m \cdot n$$

Prop. 1.23 [modular subtraction]

Given $m, n \in \mathbb{Z}$ there is

exactly one x such that

$$m + x = n.$$

Proof:

There is such an x : let $x = n + (-m)$

$$\begin{aligned} \text{then } m + x &= m + (n + (-m)) = m + (-m + n) \\ &= (m + (-m)) + n = 0 + n = n \end{aligned}$$

There is only one such x :

$$\text{if } m+x=n \text{ and } m+y=n$$

$$\text{then } m+x = m+y \text{ (cans =)} \text{ and } \\ x=y \text{ (by prop 1.9)}$$

So... if $m+x=n$

$$\text{then } m+x=n \text{ and } m+(n+(-m))=n$$

$$\text{so } x = n+(-m).$$

$$n+(-m)$$

Definition:

$$n-m \text{ is defined as } n+(-m).$$

