Example 10.11.

$$(65,\ 70) = (5 \cdot 13,\ 5 \cdot 14) = 5\,(13,\ 14) = 5 \cdot 1 = 5,$$

and hence

$$(130,\ 140) = (2 \cdot 65,\ 2 \cdot 70) = 2\,(65,\ 70) = 2 \cdot 5 = 10.$$

Corollary 10.12. *If $a,\ b \in \mathbb{N}$ and $c \in \mathbb{Z}$ satisfy $a \,|\, bc$ and $(a,\ b) = 1$, then $a \,|\, c$.*

Proof Since $(a,\ b) = 1$, Theorem 10.6 (iii) gives that there exist $x,\ y \in \mathbb{Z}$ such that $ax+by = 1$. Hence

$$acx + bcy = c.$$

Since $a \,|\, bc$, there exists $k \in \mathbb{Z}$ such that $bc = ak$. Hence

$$c = acx + aky = a\,(cx + ky)\,,$$

giving that $a \,|\, c$. □

Example 10.13. We have that $3 \,|\, 30$ and $(3,\ 5) = 1$. Hence $3 \,|\, 6$.

Definition 10.14. If $a,\ b \in \mathbb{N}$ satisfy $(a,\ b) = 1$, then we say that a is *coprime* to b.

Definition 10.15. Let $a,\ b \in \mathbb{N}$. A *least common multiple* of $a,\ b$ is an element $m \in \mathbb{N}$ such that

(M1) $a \,|\, m$ and $b \,|\, m$;

(M2) if $n \in \mathbb{N}$ satisfies $a \,|\, n$ and $b \,|\, n$, then $m \,|\, n$.

In this case we write $m = \operatorname{lcm}(a,\ b)$, which we abbreviate to $m = [a,\ b]$ if there is no ambiguity caused by doing so.

Theorem 10.16. *Pick $a,\ b,\ k \in \mathbb{N}$. Then*

(i) *$[a,\ b]$ is unique;*

(ii) *$[ka,\ kb] = k\,[a,\ b]$;*

(iii) *$(a,\ b)\,[a,\ b] = ab$.*

Proof (i) Suppose that $m,\ m' \in \mathbb{N}$ satisfy (M1) and (M2) in Definition 10.15. Then $m \,|\, m'$ and $m' \,|\, m$. Hence $m = m'$.

(ii) Let $m = [a,\ b]$. Since $a \,|\, m$ and $b \,|\, m$, so $ka \,|\, km$ and $kb \,|\, km$.

Let $m' = [ka,\ kb]$. Then, since $ka \,|\, km$ and $kb \,|\, km$, so $m' \,|\, km$.

On the other hand, $ka \,|\, m'$ and $kb \,|\, m'$. So $km \,|\, m'$. Hence $km \,|\, m'$ and $m' \,|\, km$, giving that $m' = km$.