Proposition 2.1.5. Let a and b be integers, not both zero. Then any common divisor of a and b is a divisor of $\gcd(a, b)$.

Proof. The cast of characters in this proof:

- Integers a and b such that $\boxed{a^2 + b^2 > 0}$.
- By Proposition 1.3.8 there exists a greatest common divisor of a and b. Set $g = \gcd(a, b)$.
- An integer c such that $\boxed{c|a}$ and $\boxed{c|b}$.
- The previous line gives rise to two more characters: The integers u and v such that $\boxed{a = cu}$ and $\boxed{b = cv}$. The previous line gives also more information about c: $\boxed{c \neq 0}$.

The quest in this proof is $\boxed{c|g}$. Or, more specifically the quest is $\boxed{c \neq 0}$ and an integer z such that $\boxed{g = cz}$.

Now we start with the proof. By $\boxed{\text{Theorem 2.1.3}}$ there exist integers x and y such that

$$\boxed{ax + by = g}.$$

This is a quite dramatic scene, and the characters u and v demand the stage:

$$\boxed{(cu)x + (cv)y = g}.$$

But, the associativity of multiplication yields

$$\boxed{c(ux) + c(vy) = g},$$

and distributive low now gives

$$\boxed{c(ux + vy) = g}.$$

At this point our quest is finished in a color coordinated solution

$$z = ux + vy.$$

Since also $\boxed{c \neq 0}$, the quest is successfully completed. □

Proposition 2.1.7. Let a and b be positive integers. Then any common multiple of a and b is a multiple of $\operatorname{lcm}(a,b)$.

Proof. The cast of characters in this proof:

(I) Positive integers a and b.

(II) By Proposition 1.3.9 there exists a least positive common multiple of a and b. Set $m = \operatorname{lcm}(a,b)$.

(III) The previous line, that is the phrase common multiple hides two more characters: the integers j and k such that $m = aj$ and $m = bk$.

(IV) It is important to notice the following character feature of m: It is the least positive common multiple of a and b. What this means is the following

$$\boxed{\text{If an integer } x \text{ is a common multiple of of } a \text{ and } b \text{ and } x < m, \text{ then } x \leq 0.}$$

(V) An integer c which is a common multiple of a and b.

(VI) The previous line gives rise to two more characters: The integers u and v such that $c = au$ and $c = bv$.

The quest in this proof is $m|c$. Or, more specifically the quest is $m \neq 0$ and an integer z such that $c = mz$.

Now we start with the proof. In fact we start with a brilliant idea to use Proposition 1.4.1. This proposition is applied to the integers c and $m > 0$. By Proposition 1.4.1 there exist integers q and r such that

$$\boxed{c = mq + r} \qquad \text{and} \qquad \boxed{0 \leq r \leq m-1}.$$

What we learn about r from the previous line is that $r < m$. But, there is more action waiting to be unfolded here. Follow the following two sequences of equalities (all the green equalities!):

$$r = c - mq = au - mq = au - (aj)q = a(u - jq)$$
$$r = c - mq = bv - mq = bv - (bk)q = b(v - kq).$$

The conclusion is: r is a common multiple of a and b. But wait, also $r < m$. Now the item (IV) in the cast of characters (in fact the character feature of m) implies that $r \leq 0$. Since also $r \geq 0$, we conclude $r = 0$. Going back to the equality $c = mq + r$, we conclude that $c = mq$. At this point our quest is completed in a color coordinated solution

$$z = q.$$

□

Proposition 2.1.10. If a and b are positive integers, then $ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$.

Proof. The cast of characters in this proof:

(I) Positive integers a and b.

(II) By Proposition 1.3.9 there exists a least positive common multiple of a and b. Set $m = \mathrm{lcm}(a,b)$.

(III) The previous line, that is the phrase common multiple hides two more characters: the integers j and k such that $m = aj$ and $m = bk$.

(IV) It is important to notice the following character feature of m: It is the least positive common multiple of a and b. What this means is the following

$$\text{If an integer } x \text{ is a common multiple of of } a \text{ and } b \text{ and } x > 0, \text{ then } m \leq x.$$

(V) By Proposition 1.3.8 there exists a greatest common divisor of a and b. Set $g = \gcd(a,b)$.

(VI) The previous line gives rise to two more characters: The integers u and v such that $a = gu$ and $b = gv$. Since $a > 0$, $b > 0$ and $g > 0$, we conclude that $u > 0$ and $v > 0$.

The quest in this proof is simple $ab = mg$.
Now we start with the proof. Consider a new green integer $c = guv$. Clearly

$$c = guv = av \quad \text{and} \quad c = guv = bu.$$

Hence $c = av$ and $c = bu$. That is c is a common multiple of a and b. Moreover, $c > 0$. Now the item (IV) in the cast of characters (in fact the character feature of m) implies that $m \leq c$. Hence $m \leq guv$. Multiplying both sides of this inequality by $g > 0$ we get

$$mg \leq guvg = gugv = ab.$$

Hence $mg \leq ab$. This is in some sense one half of the quest. For the second half, we recall Theorem 2.1.3 and conclude that there exist integers x and y such that

$$ax + by = g.$$

Multiplying both sides of this equality by $m > 0$ we get $mg = max + mby$. Now more characters are demanding the scene:

$$mg = max + mby = (bk)ax + (aj)by = ab(kx) + ab(jy) = ab(kx + jy).$$

Since $mg > 0$ and $ab > 0$, I conclude $kx + jy > 0$. Therefore $mg \geq ab$. This is the second half of the quest. So, the quest is completed. $\square$