Definition 1. Given two integers a and b, a number s is the *greatest common divisor* of a and b if (1) s divides both a and b, and (2) given any integer t, if t is a common divisor of a and b, then t also divides s. In symbols;

1. $s \mid a \wedge s \mid b$
2. $\forall t \in \mathbb{Z} : (t \mid a \wedge t \mid b) \implies t \mid s$

Theorem 1. Every pair of non-zero integers has a *greatest common divisor*. Furthermore, if $t = \gcd(a, b)$, then this number t can be expressed as a *linear combination* of a and b. That is,

$$t = xa + yb \quad \text{for some } x, y \in \mathbb{Z}.$$

Proof. Let J be the set of all linear combinations of a and b.

$$J = \{xa + yb \mid x, y \in \mathbb{Z}\}$$

Since $a, b, x, y \in \mathbb{Z}$, it follows that J is a subset of $\mathbb{Z}$. In fact, J is an *ideal* of $\mathbb{Z}$. To show this, we need to verify three conditions;

Condition 1. J is closed under addition:

$$(x_1a + y_1b) + (x_2a + y_2b) = (x_1 + x_2)a + (y_1 + y_2)b$$

which is in J since both $(x_1 + x_2)$ and $(y_1 + y_2)$ are in $\mathbb{Z}$.

Condition 2. J is closed under inverses:

$$-(xa + yb) = (-x)a + (-y)b$$

which is in J as well, since $-x, -y \in \mathbb{Z}$.

Condition 3. J absorbs products:

$$z(xa + yb) = (zx)a + (zy)b$$

where z is an integer, and therefore so are zx and zy.

Every ideal of $\mathbb{Z}$ is principal. If J is principal, this means that $J = \langle p \rangle$ for some $p = qa + rb$, where $q, r \in \mathbb{Z}$. Therefore p divides any element of J, and a and b are in J, so

$$p \mid a \quad \text{and} \quad p \mid b.$$

In other words, p is a common divisor of a and b. Next, to show that p is also the *greatest* common divisor; if u is a common divisor of a and b, then $a = ku$ and $b = lu$ for some integers k, and l. Then

$$p = qa + rb = qku + rlu = u(qk + rl)$$

which means that u divides p. So, p is indeed the *gcd* of a and b. $\square$