Definition 1 (Ideal)**.** Given a commutative ring R, an *ideal* of R is a subset $I \subseteq R$ which satisfies the following conditions;

1. I is closed under addition; $\forall x, y \in I : x + y \in I$
2. I is closed with respect to inverses; $\forall x \in I : (-x) \in I$
3. I absorbs products; $\forall x \in I, z \in R : xz \in I$

Definition 2 (Principal ideal)**.** An ideal P of a ring R is called a *principal ideal* when there is some element a in R, such that

$$P = aR = \{ar : r \in R\}.$$

We say that the ideal P is *generated by* the element a, and use the notation $P = \langle a \rangle$.

Lemma 1. Every ideal of $\mathbb{Z}$ is principal. (Another way to express this is to say that the integers form a *principal ideal domain*, or PID.)

Proof. Let $I \subseteq \mathbb{Z}$ be an ideal. If $I = \{0\}$, then I is the principal ideal generated by 0. If $I \neq \{0\}$, then let m be the least positive element of I. We will find that $I = \langle m \rangle$. First, we know that $\langle m \rangle \subseteq I$, since $\langle m \rangle = \{mz : z \in \mathbb{Z}\}$ and $xz \in I$ for all $x \in I, z \in \mathbb{Z}$ (by the absorption property). Next, given an arbitrary element $n \in I$, applying Euclidean division we can write

$$n = mq + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. So, $r = n - mq \in I$. It then immediately follows that $r = 0$, since $r < m$, and m is the least positive element of I. Therefore, $n = mq + 0 = mq \in \langle m \rangle$, and since n was chosen arbitrarily; if an element is in I, then it is in $\langle m \rangle$. This is the same as saying that $I \subseteq \langle m \rangle$, and we conclude that $I = \langle m \rangle$. $\square$

Definition 3. 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.

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

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 verify the three conditions;

1. J is closed under addition:

   $$(x_1 a + y_1 b) + (x_2 a + y_2 b) = (x_1 + x_2)a + (y_1 + y_2)b$$

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

2. J is closed under inverses:

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

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

3. J absorbs products:

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

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

Lemma 1 establishes that every ideal of $\mathbb{Z}$ is principal. If J is principal, this means that $J = \langle p \rangle$ for some $p = qa + rb$, where $q, r \in \mathbb{Z}$. Since p divides every element of J, and $a = 1a + 0b$ and $b = 0a + 1b$ are in J,

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

In other words, p is a common divisor of a and b. Next, to show that p is 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. $\square$