COMMON DIVISORS OF LINEAR COMBINATION OF INTEGERS

Link to: physicspages home page.

To leave a comment or report an error, please use the auxiliary blog and include the title or URL of this post in your comment.

Post date: 31 August 2025.

Theorem 1. *If d divides a and d divides b, then d divides any linear combination of a and b.*

Proof. Given that $d|a$ and $d|b$, then for some integers x and y:

$$\begin{aligned} a &= xd \\ b &= yd \end{aligned} \tag{1}$$

A linear combination of a and b can be written, with u and v being integers:

$$ua+vb = uxd+vyd \tag{2}$$

$$= (ux+vy)\,d \tag{3}$$

Since $d|\,(ux+vy)\,d$, $d|\,(ua+vb)$, so any divisor of two integers also divides any linear combination of them. $\square$

Example 1. Consider $a=9$, $b=27$. Common divisors of a and b are 1, 3 and 9. A linear combination of a and b is $9u+27v$, which is also divisible by 1, 3 and 9. Note that this is a different question from asking if we can write a common divisor as a linear combination of a and b. Bézout's lemma provides the method by which this can be calculated, and a corollary also guarantees that the greatest common divisor is the only divisor that can be written as a linear combination of a and b. In this case, $\gcd(9,27)=9$ and $9=1\times 9+0\times 27$. If we try to express the common divisor 3 as a linear combination of 9 and 27, we see from the theorem about linear Diophantine equations that this is not possible. We would be trying to solve the equation

$$9x+27y=3 \tag{4}$$

If a solution existed, the condition $\gcd(9,27)\,|3$ would have to be satisfied, and since $9\nmid 3$, no solution exists.

Example 2. Show that $\gcd(a,a+1)=1$. From the corollary of Bézout's lemma, the gcd is the only divisor that can be written as a linear combination of a and $a+1$. Since 1 is a divisor of any pair of integers, and we can write

$$-a+(a+1)=1 \tag{5}$$

then $\gcd(a,a+1)=1$.