4. Linear Combinations

Definition 1. *Let a, b be integers. Any expression of the form $ax + by$ where $x, y \in \mathbb{Z}$ is called a* **linear combination** *of a and b.*

For example, let $a = 4$ and $b = 7$. Some linear combinations of 4 and 7 are:

$$\begin{aligned}
0 &= 4(0) + 7(0) \\
4 &= 4(1) + 7(0) \\
7 &= 4(0) + 7(1) \\
11 &= 4(1) + 7(1) \\
15 &= 4(2) + 7(1) \\
1 &= 4(2) + 7(-1) \\
-3 &= 4(-2) + 7(1) \\
-4 &= 4(-1) + 7(0)
\end{aligned}$$

In fact, it is easy to see that since 1 is a linear combination of 4 and 7 then *every* integer is a linear combination of 4 and 7: Let m be an integer. Then multiplying the equation $1 = 4(2) + 7(-1)$ by m, we have $m = 4(2m) + 7(-m)$, showing that m is indeed a linear combination of 4 and 7.

Exercises:

1. Let a and b be integers (not both zero) and $d = \gcd(a, b)$. Must d divide every linear combination of a and b?

2. Suppose u and v are linear combinations of a and b. Show that any linear combination of u and v is a linear combination of a and b.

Proposition 2. *Let a and b be integers (not both zero). Then $\gcd(a, b)$ is a linear combination of a and b.*

Proof. Consider the equations in the Euclidean algorithm:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_n + 0
\end{aligned}$$

We will show by PCI that each remainder r_i, for $1 \leq i \leq n$, is a linear combination of a and b. Since $r_1 = a + b(-q_1)$, we see that r_1 is a linear combination of a and b. Let $k > 1$ and assume that r_i is a linear combination of a and b for all $i < k$. Now, from the kth equation in the algorithm, we have $r_k = r_{k-2} - r_{k-1}q_k$. That is, r_k is a linear combination of r_{k-2} and r_{k-1}. By the induction hypothesis, we know that r_{k-1} and r_{k-2} are linear combinations of a and b. Thus, by the exercise above, this means that r_k is a linear combination of a and b. By PCI, this proves that each remainder is a linear combination of a and b. In particular, this holds for $r_n = \gcd(a, b)$. □

The above proof is actually constructive. That is, it can be used to find integers x and y such that expressing $\gcd(a, b) = ax + by$. One first uses the Euclidean Algorithm to find the gcd, and then go back through each step (starting from the top) to write the remainders as linear combinations of a and b. We illustrate with the following example.

Example: Express $\gcd(141, 120)$ as a linear combination of 141 and 120.

Solution: Using the Euclidean algorithm on 141 and 120, we get

$$\begin{aligned} 141 &= 120(1) + 21 \\ 120 &= 21(5) + 15 \\ 21 &= 15(1) + 6 \\ 15 &= 6(2) + 3 \\ 6 &= 3(2) + 0, \end{aligned}$$

so $\gcd(141, 120) = 3$. We now use "back substitution" to write each of the remainders as linear combinations of 141 and 120. Most students find it helpful to use variables (usually a and b) for 141 and 120 to keep track of the 141's and the 120's in the equations. So we start by letting $a = 141$ and $b = 120$ and substitute these letters into the first equation above. Then we find the remainder as a linear combination of a and b and substitute into the next equation in the Euclidean Algorithm. We keep doing this until we reach the gcd.

$$\begin{aligned} a = b + 21 &\implies 21 = a - b \\ b = (a - b)(5) + 15 &\implies 15 = 6b - 5a \\ a - b = (6b - 5a)(1) + 6 &\implies 6 = 6a - 7b \\ 6b - 5a = (6a - 7b)(2) + 3 &\implies 3 = 20b - 17a \end{aligned}$$

Thus, we have $3 = 141(-17) + 120(20)$. (You should always check your answer at this point.)

Exercises:

1. Express $\gcd(878, 421)$ as a linear combination of 878 and 421.
2. Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. Prove that an integer m is a linear combination of a and b if and only if $d \mid m$.

Homework:

1. Express $\gcd(573, 366)$ as a linear combination of 573 and 366.
2. Suppose $d = \gcd(a, b)$ and e is any common divisor of a and b. We know that $e \le d$. Must $e \mid d$?
3. Let a and b be integers, not both zero. Prove that $\gcd(a, b) = 1$ if and only if $1 = ax + by$ for some $x, y \in \mathbb{Z}$.
4. Let a, b, d, x, y, d be integers such that $d = ax + by$, and $d > 0$. Must $d = \gcd(a, b)$?