Greatest Common Divisors

R. C. Daileda

September 1, 2020

The Fundamental Theorem of Arithmetic (FTA) completely describes the multiplicative structure of $\mathbb{Z}$. It asserts that every (positive) integer $n \geq 2$ can be uniquely expressed as a product of prime numbers. Uniqueness in the FTA is, essentially, a consequence of a result known as Euclid's Lemma, which in turn follows from what we will call Bézout's Lemma. The latter is concerned with a certain relationship satisfied by greatest common divisors of pairs of integers, a concept we now introduce.

Definition 1. Let $a, b \in \mathbb{Z}$. We define their *greatest common divisor* (GCD) to be

$$\gcd(a,b) = (a,b) = \max\{c \in \mathbb{N} \mid c|a \text{ and } c|b\}$$

provided a and b aren't both zero. We define $\gcd(0,0) = (0,0) = 0$. ▲

Remark 1.

- Note that since the set defining (a,b) is bounded by $\max\{|a|,|b|\}$ ($\min\{|a|,|b|\}$ if a and b are both nonzero), the GCD always exists.
- For any $a \in \mathbb{Z}$, $(a,0) = |a|$.
- Clearly $(a,b) = (b,a)$.
- $(8,76) = 4$, $(91,70) = 7$, $(72,84) = 12$, $(54,39) = 3$, $(16,69) = 1$

▼

The fundamental property of the GCD that we will need is the following.

Lemma 1. *Let $a, b \in \mathbb{Z}$. For any $n \in \mathbb{Z}$*

$$(a,b) = (a, b+na).$$

Proof. If $a = 0$, there is nothing to prove. So we assume $a \neq 0$. It therefore suffices to prove that

$$\underbrace{\{c \in \mathbb{N} \mid c|a \text{ and } c|b\}}_{A} = \underbrace{\{c \in \mathbb{N} \mid c|a \text{ and } c|b+na\}}_{B}.$$

Let $c \in A$. Then $c|a$ and $c|b$, so that c divides the linear combination $b + na$. Hence $c \in B$ and $A \subseteq B$. Now let $c \in B$. Since $c|a$ and $c|b+na$, c divides the linear combination $(b+na)+(-n)a = b$. So $c \in A$ and $B \subseteq A$. Therefore $A = B$ and the proof is complete. □

Remark 2. The lemma shows that, as a function of b, (a, b) is periodic with period a. ▼

We can now connect the GCD with the Division Algorithm.

Corollary 1. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Write $b = qa + r$ as in the Division Algorithm. Then*

$$(a, b) = (r, a).$$

Proof. According to the lemma we have

$$(a, b) = (a, qa + r) = (a, r) = (r, a).$$

□

We will now develop an efficient algorithm for computing (a, b). Given nonzero $a, b \in \mathbb{Z}$, consider the following sequence of divisions:

$$\begin{aligned}
b &= q_1 a + r_1, & 0 &\le r_1 < |a|, \\
a &= q_2 r_1 + r_2, & 0 &\le r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3, & 0 &\le r_3 < r_2, \\
r_2 &= q_4 r_3 + r_4, & 0 &\le r_4 < r_3, \\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1}, & 0 &\le r_{k+1} < r_k, \\
&\vdots \\
r_{n-1} &= q_{n+1} r_n, & r_{n+1} &= 0.
\end{aligned} \tag{1}$$

Because $r_k \in \mathbb{N}_0$ and $r_1 > r_2 > r_3 > \cdots$, we are guaranteed that eventually $r_k = 0$. Notice that according to Corollary 1

$$(a, b) = (r_1, a) = (r_2, r_1) = (r_3, r_2) = \cdots = (r_{n+1}, r_n) = (0, r_n) = r_n,$$

i.e. *the last nonzero remainder is equal to* (a, b). So we can compute (a, b) through repeated application of the Division Algorithm. This process is known as *the Euclidean Algorithm.*

Example 1. Let's use the Euclidean Algorithm to compute $(336, 726)$. We have

$$\begin{aligned}
726 &= 2 \cdot 336 + 54, \\
336 &= 6 \cdot 54 + 12, \\
54 &= 4 \cdot 12 + 6, \\
12 &= 2 \cdot 6.
\end{aligned}$$

The last nonzero remainder is 6. Hence

$$(336, 726) = 6.$$

◆

The quotients q_k in the Euclidean Algorithm appear to play no role in the computation of (a, b). However, if we reformulate the Euclidean Algorithm as a two-dimensional linear recursion, we will discover that the quotients yield a "hidden" relationship between a, b and (a,b). Let

$$\mathbf{x}_0 = \begin{pmatrix} b \\ a \end{pmatrix}, \mathbf{x}_1 = \begin{pmatrix} a \\ r_1 \end{pmatrix}, \mathbf{x}_k = \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} \text{ for } k \geq 2$$

and

$$Q_k = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \text{ for } k \geq 1.$$

Notice that according to equation (1)

$$\mathbf{x}_{k+1} = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k-1} - q_{k+1} r_k \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix} \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = Q_{k+1}\mathbf{x}_k$$

for all $k \geq 0$. We therefore have

$$\begin{aligned} \mathbf{x}_n &= Q_n \mathbf{x}_{n-1} \\ &= Q_n Q_{n-1} \mathbf{x}_{n-2} \\ &\vdots \\ &= Q_n Q_{n-1} \cdots Q_1 \mathbf{x}_0. \end{aligned}$$

Equivalently

$$Q_n Q_{n-1} \cdots Q_1 \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} * \\ (a,b) \end{pmatrix}. \tag{2}$$

If we write

$$Q_n Q_{n-1} \cdots Q_1 = \begin{pmatrix} * & * \\ s & r \end{pmatrix},$$

then equation (2) implies that $(a,b) = ra + sb$. We have just proven the following result.

Theorem 1 (Bézout's Lemma)**.** *Let $a, b \in \mathbb{Z}$. There exist $r, s \in \mathbb{Z}$ so that*

$$(a,b) = ra + sb.$$

Remark 3.

- Note that the Euclidean Algorithm produces the matrices Q_k thereby allowing us to compute r and s in Bézout's Lemma explicitly. Although the mere existence of r and s is sufficient for our purposes now, later on we will need to know how to actually find them, and the technique above is the most efficient way to do so.

- On the other hand, the "standard" proof of Bézout's Lemma presented in most textbooks is nonconstructive. One argues that the least element of

$$\mathbb{N} \cap \{ra + sb \,|\, r, s \in \mathbb{Z}\}$$

  is (a,b). This proves that $(a,b) = ra + sb$ for some $r, s \in \mathbb{Z}$, but gives no indication as to how such a pair might be found.

- r and s are *not unique*. For example, one can replace a given pair r, s with $r + mb$, $s - ma$ for any $m \in \mathbb{Z}$.

▼

Example 2. In the course of applying the Euclidean Algorithm to the computation of $(336, 726)$ we found that $q_1 = 2$, $q_2 = 6$ and $q_3 = 4$. Hence

$$Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}, Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}, Q_3 = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}$$

so that

$$Q_3Q_2Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -6 & 13 \\ 25 & -54 \end{pmatrix}.$$

Hence we can take $r = -54$ and $s = 25$ in Bézout's Lemma. That is

$$-54 \cdot 336 + 25 \cdot 726 = (336, 726) = 6.$$

♦

Note that in general we don't require the final line of the Euclidean Algorithm when computing r and s in Bézout's Lemma via the procedure above.

We now turn to our first application of Bézout's Lemma, which is the classification of the set of linear combinations of a given pair of integers. We introduce the following notation. Given $a \in \mathbb{Z}$, let $a\mathbb{Z}$ denote the set of multiples of a:

$$a\mathbb{Z} = \{an \,|\, n \in \mathbb{Z}\}.$$

That is, $a\mathbb{Z}$ is the set of integers divisible by a. And for $S, T \subset \mathbb{Z}$, let

$$S + T = \{s + t \,|\, s \in S, t \in T\}.$$

Notice that in this notation, $a\mathbb{Z} + b\mathbb{Z}$ is then the set of linear combinations of a and b.

Theorem 2. *Let $a, b \in \mathbb{Z}$. Then*

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}.$$

In other words, the multiples of (a, b) coincide with the linear combinations of a and b.

Proof. Since (a, b) divides both a and b, (a, b) divides every linear combination of (a, b). So every element of $a\mathbb{Z} + b\mathbb{Z}$ is a multiple of (a, b). That is,

$$a\mathbb{Z} + b\mathbb{Z} \subseteq (a, b)\mathbb{Z}.$$

Now let $c \in (a, b)\mathbb{Z}$. Then $c = (a, b)d$ for some $d \in \mathbb{Z}$. Use Bézout's Lemma to write $(a, b) = ra + sb$, with $r, s \in \mathbb{Z}$. Then

$$c = (a, b)d = (ra + sb)d = (ra)d + (sb)d = (rd)a + (sd)b \in a\mathbb{Z} + b\mathbb{Z}.$$

This shows that $(a, b)\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$ and finishes the proof.

□