Greatest Common Divisors

R. C. Daileda

January 17, 2018

We have seen that every natural number possesses a factorization into prime numbers. In order to prove that every such factorization is unique (up to the order of the factors) we need to introduce the notion of greatest common divisor.

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

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

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 $\max\{|a|,|b|\}$, the GCD always exists.
- For any $a \in \mathbb{Z}$, $(a,0) = |a|$.
- If $p \in \mathbb{N}$ is prime, then
$$(a,p) = \begin{cases} p & \text{if } p|a, \\ 1 & \text{if } p \nmid a. \end{cases}$$
- If $(a,b) = 1$ we say that a and b are *relatively prime*.
- 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 $a = b = 0$, there is nothing to prove. Otherwise it suffices to prove that

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

Let $c \in A$. Then $c|a$ and $c|b$, so that $c|b+na$ by HW. Hence $c \in B$ and $A \subseteq B$. Now let $c \in B$. Since $c|a$ and $c|b+na$, $c|(b+na)+(-n)a = b$ by HW again. 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 will now develop an efficient algorithm for computing (a, b). Our main tool will be the Division Algorithm, which we now recall.

Theorem 1 (The Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$ so that*

$$b = qa + r \text{ and } 0 \leq r < |a|.$$

Sketch. The set

$$\mathbb{N}_0 \cap \{b - qa \mid q \in \mathbb{Z}\}$$

is nonempty so it has a least element r by the Well Ordering Principal. One can show that $r \geq |a|$ contradicts minimality. Hence $0 \leq r < |a|$ and $b - qa = r$ (or $b = qa + r$), establishing existence. If we also have $b = q'a + r'$ with $0 \leq r' < |a|$, then $(q' - q)a = r - r'$ so that $a | r - r'$. But $|r - r'| < |a|$ so we must have $r - r' = 0$ and hence $q = q'$. This proves uniqueness. □

Remark 3. One can also give an inductive proof of the Division Algorithm which shows that the familiar process of long division yields q, the *quotient* and r, the *remainder*. ▼

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

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

□

Given nonzero $a, b \in \mathbb{Z}$, consider the following sequence of divisions:

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

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

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

♦

We can reformulate the Euclidean Algorithm as a two-dimensional linear recursion. 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 2 (Bézout's Lemma)**.** *Let $a, b \in \mathbb{Z}$. There exist $r, s \in \mathbb{Z}$ so that*

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

Remark 4.

- 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

$$Q_3 Q_2 Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -6 & 13 \\ 25 & -54 \end{pmatrix}.$$

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.

Lemma 2. *Let $a, b, c \in \mathbb{Z}$. If $a|bc$ and $(a, b) = 1$, then $a|c$.*

Proof. Write $1 = ra + sb$ and $bc = ad$. Then $c = rac + sbc = rac + sad = a(rc + sd)$ so that $a|c$. □

Corollary 2 (Euclid's Lemma)**.** *Let p be a prime number and $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.*

Proof. Since p is prime, if $p \nmid a$ then $(a, p) = 1$. Then by the lemma, $p|b$. □

Corollary 3 (Extended Euclid's Lemma)**.** *Let p be a prime number and $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. If $p|a_1 a_2 \cdots a_k$, then $p|a_i$ for some i.*

Proof. This is a straightforward induction using Euclid's Lemma as the base case and is left as an exercise. □

Lemma 3. *Let $p, q_1, q_2, \ldots, q_k$ be prime numbers. If $p|q_1 q_2 \cdots q_k$, then $p = q_i$ for some i.*

Proof. By the Extended Euclid's Lemma, $p|q_i$ for some i. Since $p \neq 1$ and q_i is prime, this implies $p = q_i$. □

Theorem 3 (Uniqueness of Prime Factorizations)**.** *Suppose that* $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots q_\ell$ *are prime numbers such that*

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell.$$

Then $k = \ell$ *and, after reordering if necessary,* $p_i = q_i$ *for all* i*.*

Proof. Without loss of generality we may assume that $k \leq \ell$. Since $p_1 | q_1 q_2 \cdots q_\ell$, Lemma 3 implies that $p_1 = q_i$ for some i. After reordering and relabeling, we may assume that $p_1 = q_1$. Cancelling $p_1 = q_1$ from both sides yields

$$p_2 \cdots p_k = q_2 \cdots q_\ell.$$

Repeating the preceding argument with p_2, then p_3, etc. we find that, after relabelling, $p_i = q_i$ for all $i \leq k$, and if $k > \ell$, we arrive at the equation

$$1 = q_{k+1} \cdots q_\ell.$$

Since this is clearly impossible, we must have $k = \ell$ and the theorem is proven. □