Chapter 16 - The Euclidean Algorithm

Recall:

Let a, b be integers, not both zero. The greatest common divisor of a and b, denoted $\gcd(a,b)$, is

$$\gcd(a,b) = \max \left\{ d \in \mathbb{Z} \;\middle|\; \begin{array}{l} d \text{ divides } a \text{ and} \\ d \text{ divides } b \end{array} \right\}.$$

When the meaning is clear from the context we often write (a,b) for $\gcd(a,b)$.

Is there a better way to find the "gcd" than just listing all the divisors of a and all the divisors of b?

↳ Yes! There is a much better way.

Note:

$$\gcd(a,0) = a \quad \text{and}$$

$$\gcd(-a,b) = \gcd(a,b) \leftarrow \text{since } d \mid a \text{ iff } d \mid -a$$

so we only worry about $a, b > 0$.

The key ideas are captured in the following two lemmas.

Lemma 16.1.1: Let $a, b \in \mathbb{Z}$, $b > 0$.

If $b \mid a$ then $\gcd(a,b) = b$.

Proof: If $b \mid a$, then b is a common divisor of a and b (b divides itself). But nothing larger than b can divide b, so $b = \gcd(a,b)$. $\square$

But what if $b \nmid a$, as will usually be the case?

→ Then we write $a = bq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b$, and use the following lemma.

Lemma 16.1.2: For $a, b \in \mathbb{Z} - \{0\}$, if $a = bq + r$ with $q, r \in \mathbb{Z}$ then $\gcd(a,b) = \gcd(b,r)$.

Proof: Let $a, b \in \mathbb{Z} - \{0\}$ and suppose $a = bq + r$ with $q, r \in \mathbb{Z}$. Then if d is a common divisor of b and r then d

is also a divisor of $a = \underline{\underline{b}}q + \underline{\underline{r}}$, and hence d is a common divisor of a and b.

On the other hand, if d is a common divisor of a and b then d divides $r = \underline{\underline{a}} - \underline{\underline{b}}q$ and hence d is a common divisor of b and r.

So

$$\{ d \in \mathbb{Z} \mid \begin{matrix} d \text{ divides } a \text{ and} \\ d \text{ divides } b \end{matrix} \} = \{ d \in \mathbb{Z} \mid \begin{matrix} d \text{ divides } b \\ \text{and } d \text{ divides } r \end{matrix} \}$$

and hence $\gcd(a,b) = \gcd(b,r)$. $\square$

So what?

Example Application: Find $\gcd(621, 255)$.

Solution:

$$\begin{aligned}
621 &= 255 \times 2 + 111 \\
255 &= 111 \times 2 + 33 \\
111 &= 33 \times 3 + 12 \\
33 &= 12 \times 2 + 9 \\
12 &= 9 \times 1 + 3 \\
9 &= 3 \times 3 + \underline{\underline{0}} \leftarrow \text{stop}
\end{aligned}$$

By Lemma 16.1.2:

$$(621, 255) = (255, 111) = (111, 33) = (33, 12) = (12, 9)$$
$$= (9, 3) = (3, 0).$$

But $(3,0)=3$, so we get $\underbrace{(621,255)}_{\gcd(621,255)}=3$.

Note that we could also stop at $(9,3)$ and say $(9,3)=3$ (Lemma 16.1.1).

→ We have just discovered the Euclidean algorithm!

Theorem 16.1.1 (The Euclidean algorithm):

Suppose $a, b \in \mathbb{Z}$ with $a > b > 0$. The following procedure defines a finite sequence of positive integers $\underbrace{a_0, a_1, \dots, a_n}$ with $a_n = \gcd(a,b)$.

↖ such that $\boxed{a_0 > a_1 > \cdots > a_n}$

Set $a_0 = a$, $a_1 = b$.
For each natural number k, starting from 1 and increasing by 1 each time, repeat Step k until the process terminates.

Step k:

Write $a_{k-1} = a_k q_k + r_k$ where $q_k, r_k \in \mathbb{Z}$ and $0 \leq r_k < a_k$.

If $r_k = 0$, stop.

Otherwise, set $a_{k+1} = r_k$ and continue with Step $k+1$.

Note that $a_0 > a_1 > a_2 > \dots$ which is why the procedure eventually stops.

The fact that $a_n = \gcd(a,b)$ just comes from:

$$(a,b) = (a_0, a_1) = (a_1, a_2) = \cdots = (a_{n-1}, a_n) = (a_n, 0) = a_n.$$

Another Example: Find $\gcd(353, 112)$.

$$\begin{aligned}
353 &= 112 \times 3 + 17 \\
112 &= 17 \times 6 + 10 \\
17 &= 10 \times 1 + 7 \\
10 &= 7 \times 1 + 3 \\
7 &= 3 \times 2 + \boxed{1} \\
3 &= 1 \times 3 + 0
\end{aligned}
\qquad
\begin{array}{c}
\gcd(353, 112) \\ \| \\ \gcd(112, 17) \\ \| \\ \gcd(17, 10) \\ \| \\ \gcd(10, 7) \\ \| \\ \gcd(7, 3) \\ \| \\ 1
\end{array}$$

$\longrightarrow \gcd(353, 112) = 1.$

Remarks:

- The Euclidean algorithm is highly efficient. One can prove that it takes at most 5 times the number of digits in the smaller integer b.
- This algorithm and generalizations are important in many applications, including cryptography.