

Our Greatest Common Divisor vs. the Book's
a battle to the death

(Our) Definition: Given two integers a and b , not both 0, the greatest common divisor of a and b is the largest integer that is a divisor of both.

(Their) Definition: Given two integers a and b , not both 0, the greatest common divisor of a and b is the positive number d that divides both such that $c|b$ for all common divisors c of a and b .

Note how our definition is straight-forward; such a thing exists since certainly there are common divisors (1, for example) and we showed that $m|n$ implies that $m \leq |n|$, so that the set of common divisors of a and b is a non-empty finite set. On the other hand, it isn't so clear that there is a common divisor d with the property demanded in their definition.

We can use Theorem 1.1.4 and the notion of ideals to get another way to view the greatest common divisor; a way that makes it clear the two definitions above are equivalent.

First, given any two integers a and b , the set of *linear combinations*

$$I = \{ax + by : x, y \in \mathbb{Z}\}$$

is an ideal. (Check this!) Assuming further that not both a and b are zero, this ideal consists of more than just zero and by Theorem 1.1.4 it must be of the form $I = d\mathbb{Z} = \{d \cdot z : z \in \mathbb{Z}\}$ for some positive integer d . In other words, everything in I is a multiple of d , and every multiple of d is in I . Said differently, I consists of all integers divisible by d .

We claim first that d is a common divisor of a and b . To see why, note that a and b are both in I . Next, suppose c is a common divisor of a and b ; write $a = c \cdot m$ and $b = c \cdot n$. Since d itself is in I , it must be some linear combination of a and b ; write $d = a \cdot x_0 + b \cdot y_0$. Then using our basic properties

$$\begin{aligned} d &= a \cdot x_0 + b \cdot y_0 \\ &= (c \cdot m) \cdot x_0 + (c \cdot n) \cdot y_0 \\ &= c \cdot (m \cdot x_0) + c \cdot (n \cdot y_0) \\ &= c \cdot (m \cdot x_0 + n \cdot y_0). \end{aligned}$$

Thus, $c|d$. This makes d the greatest common divisor of a and b by the book's definition. But it also implies that $d \geq c$ since $d > 0$.