2. Greatest Common Divisor

Given an integer $a \in \mathbb{Z}$ one can examine all of its divisors by collecting them into a set, which we choose to notate as $\mathcal{D}(a)$. For example

$$\begin{aligned}\mathcal{D}(28) &= \{-28, -14, -7, -4, -2, -1, 1, 2, 4, 7, 14, 28\} \\ \mathcal{D}(-49) &= \{-49, -7, -1, 1, 7, 49\}\,.\end{aligned}$$

Since for every divisor $d \in \mathcal{D}(a)$ it follows that $-d \in \mathcal{D}(a)$, we can, without loss of generality, focus on the *positive divisors*:

$$\begin{aligned}\mathcal{D}_+(28) &= \{1, 2, 4, 7, 28\} \\ \mathcal{D}_+(-49) &= \{1, 7, 49\}\end{aligned}$$

Given two integers $a, b \in \mathbb{Z}$, we can explore their **common divisors** by intersecting their sets of (positive) divisors. Continuing our example where $a = 28$ and $b = -49$ we have

$$\textbf{common divisors } = \mathcal{D}_+(28) \cap \mathcal{D}_+(-49) = \{1, 7\}\,.$$

Two integers may have many common divisors or very few. For example, the integers 100 and 50 have six common divisors, while 46 and 27 have only one. If you explore some basic examples, though, you can convince yourself that 1 is *always* a common divisor, no matter which two integers a and b you pick.

Example 2.1. *Given any two integers $a, b \in \mathbb{Z}$, explain why the set of common divisors $\mathcal{D}_+(a) \cap \mathcal{D}_+(b)$ always has 1 as its smallest element.*

Given two integers, $a, b \in \mathbb{Z}$, a more interesting number to consider, then, is the ***greatest common divisor***, which we notate and precisely define as follows

$$\gcd(a, b) = \max\Big(\mathcal{D}_+(a) \cap \mathcal{D}_+(b)\Big).$$

That is (and as its name suggests), **the greatest common divisor** of two integers a and b is the largest positive number that divides both.

Example 2.2. *It follows that* $\gcd(28, -49) = 7$. *Make sure you understand the following statements:*

(1) $\gcd(100, 50) = 50$

(2) $\gcd(-95, 38) = 19$

(3) $\gcd(46, 27) = 1$

(4) $\gcd(0, 58) = 58$

(5) $\gcd\left(2^{12},\, 3^2 \cdot 5^4\right) = 1$

Note. When considering the gcd of two integers, we need to impose one minor restriction: the integers cannot *both* be zero. Indeed, take a few moments to think about the set $\mathcal{D}_+(0)$ to determine what "goes wrong" when considering $\gcd(0, 0)$.

Wait, Why Does Anyone Care About the $\gcd(a, b)$**?** The greatest common divisor has been studied for quite a while (in fact the next sub-section details Euclid's approach to computing it), and there are quite a few reasons we want math and computer science students to be aware of it and how it works.

The following example provides some insight as to why a recursive-structure-oriented computer scientist or mathematician might care about it, and there are other reasons and examples that provide alternative motivation, too.

Example 2.3. *Take any two integers, $a, b \in \mathbb{Z}$ and consider the recursively defined set S:*

$$a, b \in S$$

$$\textit{If } x, y \in S, \textit{ then } sx + ty \in S \textit{ for every } s, t \in \mathbb{Z}$$

The expression "$sx + ty$" is called a **(integer) linear combination of** *x and y. In other words, the elements of S are "built" from linear combinations of the base elements a and b.-18*

For example, if $a = 4$ and $b = 6$, then S consists of all linear combinations of these integers, so that $2 \cdot 4 + (-3) \cdot 6 = 10 \in S$ and $(-1) \cdot 4 + 5 \cdot 6 = 26 \in S$. Explore this set with lots of examples and you'll likely see that $S = \{\text{all multiples of } 2\}$.

If we use $a = 15$ and $b = 8$, then the resulting set S contains lots more elements. For instance $1 \cdot 15 + (-1) \cdot 8 = 7 \in S$ and $(-1) \cdot 15 + 2 \cdot 8 = 1 \in S$. Indeed, in this example S contains all possible integers, so that $S = \mathbb{Z}$.

When $a = 45$ and $b = 117$, the resulting set S turns out to be

$$S = \{\cdots -18, -9, 0, 9, 18, \cdots\} = \{\text{all multiples of } 9\}\,.$$

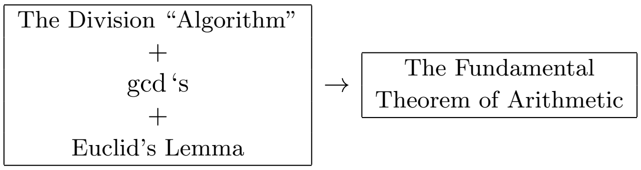
(Try lots of examples to convince yourself o this!)

There is, indeed, a pattern lurking behind the scenes here. A recursively-defined set like S always ends up "collapsing" into a set of multiples. Specifically

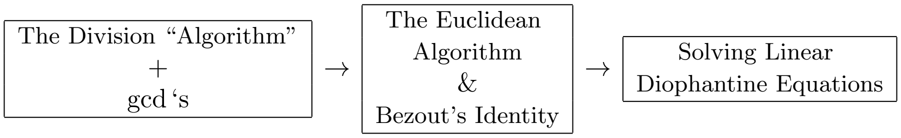
$$S = \{\text{ all multiples of } \gcd(a, b)\,\}\,.$$

Ancient Greek Mathematicians (like Euclid) were also interested in the concept of gcd because of its connection to "commensurate measurements" – that is, they wanted to understand when the lengths of two constructed line segments could be compared using rational numbers, the and greatest common divisors helped them do precisely that. Number Theorists and Algebraists later came to understand how the gcd is useful in unraveling other, more abstract ideas, too.

We include the gcd in this text because it figures prominently in many Number Theory discussions, and also because it helps us set up some key ingredients for an essential theorem about numbers that *everyone on the planet* should be familiar with, **The Fundamental Theorem of Arithmetic**. Here's how this will go:



There is another "chain of Number Theory" ideas we should show you here, too, namely



We will conclude this chapter with discussions of Modular Arithmetic and Linear Diophantine Equations, topics we save for Section 5. Sections 2 and 3 walk through the Euclidean Algorithm and Bezout's Identity, respectively, while Section 4 provides a brief but satisfying overview of the Fundamental Theorem of Arithmetic. With so many interesting ideas to connect, let's get started straight away!

The Euclidean Algorithm. Thankfully, this algorithm *is* an actual algorithm! Also called "the Euclidean Division Algorithm," its goal is not to divide two integers, $a, b \in \mathbb{Z}$, but to compute their gcd, and it is based on one key fact:

$$\gcd(a, b) = \gcd(a - b, b).$$

This property is surprisingly simple or cute to verify, and we will leave it as a guided (homework) exercise. For the time being, though, let's accept this as true and note that by **iterating this over and over** the Division "Algorithm" rears its head! If we repeat this fact q times then we find

$$\gcd(a, b) = \gcd(a - qb, b) = \gcd(r, b)$$

where, of course, r is our promised remainder and q our promised quotient. The Euclidean Division Algorithm is now easy to describe: it repeatedly applies the Division "Algorithm" to a sequence of divisors and remainders:

Euclidean Algorithm

(1) Given $a, b \in \mathbb{Z}$ with $b \neq 0$, use the Division "Algorithm" to write

$a = q_1 \cdot b + r_1$

(2) Apply the Division "Algorithm" to b and r_1 to find

$b = q_2 \cdot r_1 + r_2$

(3) Repeatedly apply the Division "Algorithm" until a remainder with value 0 is produced

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ r_2 &= q_4 \cdot r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

(4) If $r_{n+1} = 0$, then the previous remainder, r_n, is the $\gcd(a, b)$.

Note that the final step of the algorithm relies on the fact that for any integer a, $\gcd(a, 0) = a$.

We also point out the amazing fact that this Algorithm works without having to figure out the divisors of the integers a and b, which can be a life-saver when working with rather large quantities.

Example 2.4. *Use the Euclidean Algorithm to compute* $\gcd(120, 34)$.

$$\begin{aligned} 120 &= 3 \cdot 34 + 18 \\ 34 &= 1 \cdot 18 + 16 \\ 18 &= 1 \cdot 16 + 2 \\ 16 &= 8 \cdot 2 + \boxed{0} \end{aligned}$$

The Euclidean Algorithm tells us that $\gcd(120, 34) = 2$.

Example 2.5. *Use the Euclidean Algorithm to compute* $\gcd(1044, 339)$.

$$\begin{aligned} 1044 &= 3 \cdot 339 + 27 \\ 339 &= 12 \cdot 27 + 15 \\ 27 &= 1 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + \boxed{0} \end{aligned}$$

It follows that $\gcd(1044, 339) = 3$.

Example 2.6. *Use the Euclidean Algorithm to compute* $\gcd(2022, 49)$.

$$\begin{aligned} 2022 &= 41 \cdot 49 + 13 \\ 49 &= 3 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + \boxed{0} \end{aligned}$$

It follows that $\gcd(1044, 339) = 1$.

The last example above tells us something “special” happened with the integers 2022 and 49, namely their greatest common divisor also equals their *smallest* common divisor. It follows that *the only (positive) divisor that* 2022 *and* 49 *share is* 1, and we give this phenomenon a special name.

Two integers $a, b \in \mathbb{Z}$ are said to be **relatively prime** (also called **coprime**) precisely if $\gcd(a, b) = 1$. This only happens when $\mathcal{D}_+(a) \cap \mathcal{D}_+(b) = \{1\}$.