7.2 Properties of the Greatest Common Divisor

In this section, we'll take a closer look at the *greatest common divisor* of two numbers. Recall the following definitions from 7.1 Introduction to Number Theory.

Definition. Let $x, y, d \in \mathbb{Z}$. We say that d is a **common divisor** of x and y when d divides x and d divides y.

We say that d is the **greatest common divisor** of x and y when it is the largest number that is a common divisor of x and y, or 0 when x and y are both 0. We can define the function $\gcd : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ as the function which takes numbers x and y, and returns their greatest common divisor.

To make it easier to translate this statement into symbolic form, we can restate the "maximum" part by saying that if e is any number which divides m and n, then $e \leq d$. Let $m, n, d \in \mathbb{Z}$, and suppose $d = \gcd(m, n)$. Then d satisfies the following statement:

$$\begin{aligned}&\Big(m = 0 \land n = 0 \Rightarrow d = 0\Big) \land \\ &\Big(m \neq 0 \lor n \neq 0 \Rightarrow \\ &\qquad d \mid m \land d \mid n \land \big(\forall e \in \mathbb{N},\ e \mid m \land e \mid n \Rightarrow e \leq d\big)\Big)\end{aligned}$$

This expression has a few subtleties. First, because we actually have separate definitions for $\gcd(m, n)$ when both arguments are zero and when at least one of them is non-zero, these two definitions are expressed as two different implications.[1]

[1] This is analogous to writing an if statement in Python. In this case, we're saying that only one of the conclusions needs to be True, depending on which of the hypotheses are True.

Here is an example proof which makes use of both this definition, and the definition of prime.

Example. Prove that for all integers p and q, if p and q are distinct primes, then p and q are *coprime*, meaning $\gcd(p, q) = 1$.

Translation. Here is an initial translation which focuses on the structure of the above statement, but doesn't unpack any definitions:

$$\forall p, q \in \mathbb{Z},\ \big(Prime(p) \land Prime(q) \land p \neq q\big) \Rightarrow \gcd(p, q) = 1.$$

We could unpack the definitions of $Prime$ and gcd, but doing so would not add any insight at this point. While we will almost certainly end up using these definitions in the discussion and proof sections, expanding it here actually obscures the meaning of the statement.[2]

[2] In general, use translation as a way of precisely specifying the *structure* of a statement; as we have seen repeatedly, the high-level structure of a statement is mimicked in the structure of its proof. And while you don't need to expand every definition in a statement, you should *always* keep in mind that definitions referred to in the statement will require unpacking in the proof itself.

Discussion. We know that primes don't have many divisors, and that 1 is a common divisor for any pair of numbers. So to show that $\gcd(p, q) = 1$, we just need to make sure that neither p nor q divides the other (otherwise that would be a common divisor larger than 1).

Proof. Let $p, q \in \mathbb{Z}$. Assume that p and q are both prime, and that $p \neq q$. We want to prove that $\gcd(p, q) = 1$.

By the definition of prime, we know that $p \neq 1$ (since $p > 1$). Also by the definition of prime, the only positive divisors of q are 1 and q itself. So then since $p \neq q$ (our assumption) and $p \neq 1$, we know that $p \nmid q$.

Next, we know that 1 divides every number (as we proved in 4.6 Proofs and Programming I: Divisibility), and so 1 is the only positive common divisor of p and q, so $\gcd(p, q) = 1$. ∎

In the above proof, we referred to a statement we had proved to justify the final step. In general, our proofs can consist of steps which are statements that we know are true because of an external source, even one that *we don't know how to prove ourselves*.

This is a fundamental parallel between writing proofs and writing computer programs. In programming, we start with some basic building blocks of a language—data types, control flow constructs, etc.—but we often rely on libraries as well to simplify our tasks. We can use these libraries by reading their documentation and understanding how to use them, but don't need to understand how they are implemented. In the same way, we can use an external theorem in our proof by understanding what it means, but without knowing how to prove it.

Let's look at one example of this in action.

Linear combinations and the greatest common divisor

First, a "helper" definition:

Definition. Let $m, n, a \in \mathbb{Z}$. We say that a is a **linear combination of** m **and** n when there exist $p, q \in \mathbb{Z}$ such that $a = pm + qn$.

For example, 101 is a linear combination of 5 and 3, since $101 = 10 \cdot 5 + 17 \cdot 3$.

We can use this definition to state one fairly straightforward property of divisibility and one *surprising* property of the greatest common divisor.

Theorem. (*Divisibility of Linear Combinations*) Let $m, n, d \in \mathbb{Z}$. If d divides m and d divides n, then d divides every linear combination of m and n.

Theorem. (*GCD Characterization*) Let $m, n \in \mathbb{Z}$, and assume at least one of them is non-zero. Then $\gcd(m, n)$ is the smallest positive integer that is a linear combination of m and n.

Next, we'll see how to use these two theorems as "helpers" inside a proof of the following statement, which is yet another property of the greatest common divisor.

Example. For all $m, n, d \in \mathbb{Z}$, if d divides both m and n then d also divides $\gcd(m, n)$.

Translation. We can translate this statement as follows:

$$\forall m, n, d \in \mathbb{Z},\ d \mid m \land d \mid n \Rightarrow d \mid \gcd(m, n).$$

Discussion. This one is a bit tougher. All we know from the definition of gcd is that $d \leq \gcd(m, n)$, but that doesn't immediately imply that $d \mid \gcd(m, n)$!

But given the context that we just discussed in the preceding paragraphs, I'd guess that we should also use the GCD Characterization Theorem to write $\gcd(m, n)$ as $pm + qn$. Oh, and the theorem before that one said that any number that divides m and n will divide $pm + qn$ as well!

Proof. Let $m, n, d \in \mathbb{Z}$. Assume that $d \mid m$ and $d \mid n$. We want to prove that $d \mid \gcd(m, n)$. We'll divide our proof into two cases.[3]

[3] After reading the next two cases, answer: why did we need to divide our proof into cases? Is there another way we could have written this proof?

Case 1: assume $m = 0$ and $n = 0$.

In this case, by the definition of gcd we know that $\gcd(m, n) = 0$. So $d \mid \gcd(m, n)$, since we assumed that d divides m and n, which are 0.

Case 2: assume $m \neq 0$ or $n \neq 0$.

Then by the GCD Characterization Theorem, there exist integers $p, q \in \mathbb{Z}$ such that $\gcd(m, n) = pm + qn$.[4]

[4] This line uses a known external statement that is an existential to *introduce* two variables p and q to use in our proof.

Then by the the Divisibility of Linear Combinations Theorem, since $d \mid m$ and $d \mid n$ (by assumption), we know that $d \mid pm + qn$.

Therefore $d \mid \gcd(m, n)$. ∎