Divisibility

Reading

Section 3.1

Practice Problems

3.1 1, 3, 5, 7, 9, 10, 13, 16
Challenge 3.1 (optional) 8, 14, 25, 28 (and how about the converse of 28?)

Notes

Divisibility is a notion pretty much exclusive to integers (in our context).

> We say that d **divides** a, and write $d \mid a$, when there is an integer q such that $qd = a$.
>
> In other words, can we evenly multiply d into a?
>
> We also say that a is **divisible by** d or a **multiple of** d, or that d is a **divisor** or **factor** of a.

In the case where a and d are natural numbers, then q must be a natural number also.

Food for thought:

- Which numbers does 0 divide?
- Which numbers divide 0?
- Which numbers does 1 divide?
- Which numbers divide 1?
- Does a number divide itself?

Here is a simple but important result:

> If $d \mid a$ and they are both natural numbers, then $1 \leq d \leq a$.

To see this:

- As all natural numbers, $1 \leq d$.
- As $d \mid a$, we can write $a = dq$, q natural number.
- So $1 \leq q$.
- Multiply by d: $d \leq dq = a$.
- So $1 \leq d \leq a$.

This is very useful. It tells us that if we are looking for natural divisors of a natural number a, we only have to look at the numbers from 1 to a. It considerably limits our search.

The following simple lemma has very far-reaching consequences:

> If d divides both a and b, then it must also divide any **integer linear combination** of a and b, namely any number of the form $c = ma + nb$ where m, n are any integers.
>
> In particular if d divides a then it divides any multiple of a. And if it divides a, b then it also divides their sum $a + b$.

Proof:

- $a = dk_1$, $b = dk_2$.
- So $ma = dmk_1$. And $na = dnk_2$.
- Then $c = ma + nb = dmk_1 + dnk_2 = d(mk_1 + nk_2)$.
- Since the expression in parentheses is an integer, d divides c.

To see how this might be useful, suppose we want to find all the common divisors of the numbers 119 and 203. So what numbers divide into both? We already know that 1 divides into every number. What other numbers work?

- The trick is that as long as we form integer linear combinations of these numbers, the result must be divisible by any divisor of those two.
- For instance, $2 \times 119 - 203 = 35$. So whatever common divisors 119 and 203 have, then 35 must have them also.
- Now we make a linear combination of 35 and 119: $119 - 3 \times 35 = 14$. So whatever common divisors 119 and 203 have, then 35 and now 14 must have them too.
- Finally, we make a linear combination of 35 and 14: $35 - 2 \times 14 = 7$. So whatever common divisors 119 and 203 have, then 7 must have them also.
- But it is easy to see that 7 has no other natural number divisors other than 1 and 7. Therefore those are the only common divisors of 119 and 203.

This is an idea we will use a lot in the future. Starting with the numbers whose common divisors we are looking for, we keep forming linear combinations, all the time simplifying our numbers, until they become so small that we can easily figure out all their divisors. We will make this a bit more precise in a couple of days.

Here is one more consequence of this theorem:

> For any $n \geq 1$, the numbers n and $n + 1$ have no common divisor other than 1.

This follows directly from the fact that if d divides n and $n + 1$, then it must also divide $(n + 1) - n = 1$. and only 1 divides 1.

In-class: Play the divisor game