Discrete Mathematics lecture notes 2-2

September 17, 2013

9. Detour: Prelude to posets

We are familiar with the standard ordering $\leq$ on $\mathbb{N}$. This is an ordering in the sense defined last week,[1] which we should think of as arising from the *additive* structure on $\mathbb{N}$. In other words, we could define for natural numbers a and b, $a \leq b$ if there is some $c \in \mathbb{N}$ such that $b = a + c$. Check that the following properties are satisfied for all $a, b, c \in \mathbb{N}$ by this definition:

(1) $a \leq a$.

(2) If $a \leq b$ and $b \leq a$, then $a = b$.

(3) If $a \leq b$ and $b \leq c$, then $a \leq c$.

(4) $a \leq b$ or $b \leq a$.[2]

That (4) is true is basically a restatement of the Induction Axiom: Every natural number can be obtained by adding 1 to 0 enough times.[3]

What if we want to work multiplicatively instead of additively? That is, let's take our definition of $\leq$ ($a \leq b$ if there is some $c \in \mathbb{N}$ such that $b = a + c$) and modify it: Define $a \preceq b$ if there is some $c \in \mathbb{N}$ such that $b = a \cdot c$. Note that we've already seen this with slightly different notation:

$$a \preceq b \Leftrightarrow a|b.$$

How many of the ordering properties does $\preceq$ satisfy? Let $a, b, c \in \mathbb{N}$.

(1) $a \preceq a$? In other words, is $a|a$ true for all $a \in \mathbb{N}$? Clearly yes, as $a = a \cdot 1$.

(2) If $a \preceq b$ and $b \preceq a$, is it true that $a = b$? If $a \preceq b$, there is some x so that $b = a \cdot x$, and if $b \preceq a$ there is some y so that $a = b \cdot y$. Putting these together, we get

$$b = a \cdot x = (b \cdot y) \cdot x = b \cdot (xy).$$

But this implies $xy = 1$,[4] which implies $x = y = 1$, or $a = b$, so (2) is satisfied as well.

(3) If $a \preceq b$ and $b \preceq c$, is it true that $a \preceq c$? In other words, if $a|b$ and $b|c$, does $a|c$? Yes; this was one of the first results we proved in this class.

(4) Is it true that $a \preceq b$ or $b \preceq a$, for all $a, b \in \mathbb{N}$? Well, let's try $a = 2$, $b = 3$. Then $2 \nmid 3$ and $3 \nmid 2$, so (4) *does not hold*. We say in this case that 2 and 3 are *incomparable*; in that they cannot be compared.

So working multiplicatively we get something similar to, but distinct from, the standard ordering $\leq$. Because $\preceq$ satisfies (1)-(3), it is still very similar to our intuitive understanding of an ordering, but because (4) fails it cannot be a *total* ordering.

Definition 1. Let $\mathcal{P}$ be a set and $\preceq$ a relation on $\mathcal{P}$. $\preceq$ is a *partial order* if for all $x, y, z \in \mathcal{P}$:

(1) $(x \preceq y) \wedge (y \preceq x) \Rightarrow (x = y)$.[5]

(2) $(x \preceq y) \wedge (y \preceq z) \Rightarrow (x \preceq z)$.

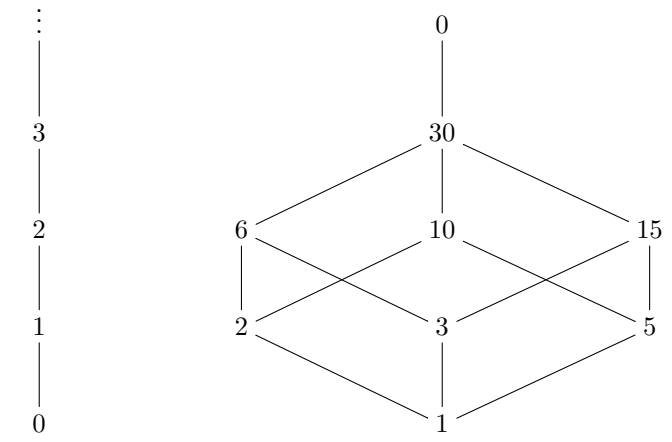
(3) $(a \preceq b) \vee (b \preceq a)$.

[1] Actually, we worked with the strict ordering $<$ last week. I claim that $<$ determines $\leq$ and conversely. Can you prove this?
[2] This is a different formulation than the trichotomy axiom from last week; what is the cause for the discrepancy?
[3] Why does this imply (4)?
[4] Actually, it doesn't. What special case am I forgetting? Can you fill in the gaps?
[5] If $\preceq$ satisfies (2) and (3) but not (1), it is a *preorder*.

The data of $\mathcal{P}$ with the partial order $\preceq$ is called a *partially ordered set*, or *poset* for short.

We will come back to general partial orderslater; for now let's just concentrate on the two[6] partial orders on $\mathbb{N}$ we've defined: The standard (additive) total order $\leq$ and the new (multiplicative) partial order $\preceq$.

Remark 2. There is a convenient way of visualizing a discrete poset $(\mathcal{P}, \preceq)$ geometrically, called a *Hasse diagram*. This is a way of arranging the elements of $\mathcal{P}$ with lines between them, where an upward line from a to b indicates that $a \prec b$[7] and there is no c such that $a \prec c \prec b$. For example, consider the Hasse diagrams for $(\mathbb{N}, \leq)$ and the subset $S = \{1, 2, 3, 5, 6, 10, 15, 30, 0\} \subseteq \mathbb{N}$ with the new partial order $\preceq$:



$(\mathbb{N}, \leq)$ $(S, \preceq)$

The Hasse diagram for $(\mathbb{N}, \leq)$, is just a vertical tower, while if you were to continue constructing the diagram for $(\mathbb{N}, \preceq)$ it would not just be infinitely tall (with 0 at the very top), but infinitely wide as well.[8]

10. Greatest Common Divisors

Let's use our new partial ordering $\preceq$ on $\mathbb{N}$ to define some basic arithmetic notions:

Definition 3. Let $a, b \in \mathbb{N}$ be two natural numbers, not both 0.

- A *common divisor* of a and b is any $c \in \mathbb{N}$ such that $c \preceq a$ and $c \preceq b$.
- A *greatest common divisor* of a and b is a common divisor of a and b, d, such that if c is any common divisor of a and b, then $c \preceq d$.

Whenever we make a new definition, the first thing we should do is check that we haven't accidentally described the empty set: We must show that the objects we've defined actually exist, or our definition isn't worth much. Moreover, when we make a definition with a word like "greatest" or "least" or any such superlative, basic grammatical decency requires us to not only prove existence, but uniqueness as well.

Theorem 4. *If $a, b \in \mathbb{N}$, not both 0, then there is a unique greatest common divisor d of a and b. This number will be denoted $GCD(a, b)$, or just (a, b) if there is no cause for confusion.*

Proof. This is another two-in-one proof, with essentially logically independent halves.

Uniqueness: Suppose that d and d' are both greatest common divisors of a and b; we want to show that $d = d'$. As d is a common divisor of a and b, the fact that d' is a GCD implies that $d \preceq d'$. Conversely, as

[6]Note that a total order is a special case of a partial order.

[7]$\prec$ is a new symbol we haven't defined yet. How would you define it in terms of $\preceq$?

[8]The bottom row of this tower is just 1, but what are the elements that would be in the second row?

d' is a common divisor of a and b, the fact that d is a GCD implies that $d' \preceq d$. Thus we have $d \preceq d'$ and $d' \preceq d$, so, as $\preceq$ is a partial order, we must have $d = d'$, as desired.

Existence: We need to construct a GCD of a and b, which should be a natural number with certain properties. At this point, we really only have one tool that asserts axiomatically the existence of natural numbers, namely the Well Ordering Principle. So let us make the unmotivated definition

$$S := \{ax + by | x, y \in \mathbb{Z} \text{ and } ax + by > 0\} \subseteq \mathbb{N}.$$

In other words, S is the collection of *strictly positive* natural numbers that can be written as an integral linear combination of a and b. Since at least one of a and b is nonzero, S is nonempty,[9], so by the well ordering of $\mathbb{N}$, S has a least element, call it d, suggestively. Since $d \in S$, there are integers x_0 and y_0 such that $d = ax_0 + by_0$.

I claim that d is a greatest common divisor of a and b. First, let us see that d is a common divisor, meaning $d \preceq a$ and $d \preceq b$. Let's focus on $d \preceq a$, or in our other notation, let's show that $d|a$.

By the Division Theorem for $\mathbb{N}$, we know that we can find unique natural numbers q, r with $0 \leq r < d$ such that

$$a = qd + r.^{10}$$

Note that if $r = 0$, we will have $d|a$, as desired. So suppose for contradiction that $r \neq 0$. We can then write

$$0 \neq r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

Since $x_0, y_0, q \in \mathbb{Z}$, we conclude that $1 - qx_0$ and $-qy_0$ are integers. Since $r > 0$, by our contrary hypothesis, we conclude that $r \in S$, and moreover $r < d$ from the conclusion of the Division Theorem. But this means that d was not actually the least element of S, contrary to how it was chosen, giving us our contradiction. Therefore we must have $r = 0$, and $d|a$.

Before we jump into proving that $d|b$, let's simply note that there is no essential difference between a and b in the above argument, and just write "$d|b$ by symmetry."[11]

So far we've proved $d|a$ and $d|b$, so that d is *a* common divisor of a and b. To show that it is a[12] GCD, let c be some other common divisor, and let's show that $c|d$. We started out writing $d = ax_0 + by_0$. Since $c|a$ and $a|ax_0$, we have $c|ax_0$. Similarly, $c|by_0$ since $c|b$. But we've already seen in the homework that if $c|u$ and $c|v$, then $c|u + v$; in this case, this simply translates to $c|d$, and the Theorem is proved. □

So far, this has been a great example of an unfortunately common phenomenon in more advanced mathematics: We are able to show the unique existence of a number with certain properties[13], but we have not actually constructed the element; we know that it exists, but we do not know what it *is*. In many cases, this is as far as we can go: It is in general impossible truly get your hands on an object defined in terms of its properties, so you just use those properties when you work with it in the future. However, in this situation fate smiles on us, for we actually have a way of computing (a, b) with an efficient algorithm. It begins with the following:

Notation 5. If $a, b \in \mathbb{Z}$ with $b > 0$, then by the Division Theorem we can write find $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and $a = qb + r$. We will write $a \mod b$ for r.

Proposition 6. *Let $a, b \in \mathbb{N}$ not both be zero. Then $(a, b) = (b, a \mod b)$.*

Proof. Set $d = (a, b)$ and $d' = (b, a \mod b)$. If we can show that $d \preceq d'$ and $d' \preceq d$, the partial ordering axioms will give us $d = d'$, as desired.

[9] Can you name one element in S?

[10] In order to apply the Division Theorem, we need for d to satisfy a certain condition. What is it, and does it obtain?

[11] If you're not convinced, you should start to write out the proof that $d|b$ and keep going until you are.

[12] Hence, "the," by the uniqueness part of the theorem.

[13] Or some other mathematical object, like a set, a group, a space, a ....

$d|d'$: Since $d' = (b, a \mod b)$, it will suffice to show that $d|b$ and $d|(a \mod b)$. $d|b$ because $d = (a, b)$. On the other hand, $(a \mod b)$ is $a - qb$ for some $q \in \mathbb{Z}$; as $d|a$ and $d|b$, it follows that $d|a = qb = a \mod b$, as claimed.

$d'|d$: Since $d = (a, b)$, it suffice to show that $d'|a$ and $d'|b$. $d'|b$ because $d' = (b, a \mod b)$. Since $d'|a \mod b$ and $a = qb + (a \mod b)$ and $d'|b$, it follows that $d'|a$, and the result is proved. □

How does this help us? Basically, computing remainders is computationally easy; our basic long division knowledge will let us do it relatively quickly.[14] Repeated applications of the previous proposition gives

$$(a, b) = (b, \underbrace{a \mod b}_{=:b_1}) = (b_1, \underbrace{b \mod b_1}_{=:b_2}) = (b_2, \underbrace{b_1 \mod b_2}_{=:b_3}) = \dots$$

Now by definition of mod as a remained, we have $b > b_1 > b_2 > b_3 > \dots$, so the set of natural numbers that occur in this manner must eventually terminate in 0, say $b_{n+1} = 0$. The last term of the equality chain is then $(a, b) = (b_n, 0) = b_n$.[15]

Try out this algorithm with a few numbers:

$$\begin{aligned}(18578903345810437, 12785) = (12785, 2032) = (2032, 593) = (593, 253)\\ = (253, 87) = (87, 79) = (79, 8) = (8, 7) = (7, 1) = (1, 0) = 1.\end{aligned}$$

Aside: When I tried to check this using an online GCD calculator, I wasn't able to find one that would accept these numbers, as the first is too big. However, it was easy for me to find an online mod -calculator, which is what I used for the computation. This should be taken as further evidence for the usefulness of this algorithm.

Definition 7. If $a, b \in \mathbb{N}$ are such that $(a, b) = 1$, then a and b are *relatively prime*.

[14] Compare: Is it faster to divide 18578903345810437 by 12785 or find all the prime factors of 18578903345810437? I'll wait.
[15] Why?