Discrete Mathematics lecture notes 2-2

September 19, 2013

11. Prime factorization

Last time we showed that any two natural numbers have a largest multiplicative piece in common—what we called the GCD—and found an efficient manner of computing this common piece. This time we'll show that this process can be continued further, so that every (nonzero) natural number can be be broken down to its atomic components, what we'll call the prime numbers:

Definition 1. A natural number p is *prime* if $p > 1$ and $n \preceq p$[1] implies $n = 1$ or $n = p$.

In other words, a natural number that is greater than 1 is prime if it has no *nontivial, proper divisors*.

The overarching claim is that, just as the number 1 generates $\mathbb{N}$ additively (every natural number can be written as a sum of 1 multiple times, and there is only one such way of writing each number), the primes generate $\mathbb{N}$ multiplicatively. More formally:

Notation 2. Let $\mathcal{P}$ denote the set of all prime numbers.

Theorem 3 (Fundamental Theorem of Arithmetic (for $\mathbb{N}$))**.** *Let $n \in \mathbb{N}$ be nonzero. Then for each $p \in \mathcal{P}$, there is a unique $\ell_p(n) \in \mathbb{N}$*[2] *such that*

$$n = \prod_{p \in \mathcal{P}} p^{\ell_p(n)}.$$

Remark 4. The symbol $\prod$ is the multiplicative analogue of $\sum$. Care to hazard a guess as to why these symbols were chosen for multiplication and addition, respectively?

Remark 5. The combined associativity and commutativity of multiplication (and addition!) is what allows us to write something like $\sum_{i=1}^{10} i^2$ or $\prod_{j=4}^{8} \frac{1}{j}$ or $\ldots$, but only if we are taking the sum or product of a *finite* number of terms.[3] However, as far as we know, the set $\mathcal{P}$ could be[4] infinite. How to reconcile?

We are really introducing a notational convention here that will make life easier as we go along: Since multiplying by the multiplicative identity 1 has no effect, we *define* multiplying by an infinite string of multiplicative identities to also have no effect. Thus, implicit in the statement of the Fundamental Theorem of Arithmetic is the assertion that $\ell_p(n) = 0$ for all but a finite number of $p \in \mathcal{P}$.

Instead of setting out to prove the Theorem directly, we will build up to it in a few small steps. This is extremely typical of how mathematical argumentation goes: In general, one isn't able to start from first principles and draw a direct chain of implication or contradiction to the truth or falsehood of the statement of a given Theorem, especially as the Theorems get more complicated. Instead, we make many small steps, each of which is easy to digest, and are often of significant use in their own right.[5] Such is the case here:

Lemma 6. *Let $p \in \mathcal{P}$ be prime and $a \in \mathbb{N}$. Then*

$$(p, a) = \begin{cases} p & p \preceq a \\ 1 & p \not\preceq a \end{cases}.$$

Proof. If $p \preceq a$ (so that $p|a$), then clearly p is a common divisor of p and a. If c is any other common divisor, then $c \preceq p$, so $c = 1$ or $c = p$ because p is prime. By inspection, we conclude that $p \preceq a$ implies $(p, a) = p$.

On the other hand, if $p \not\preceq a$ (so that $p \nmid a$), then $(p, a) \neq p$. Since $(p, a) \preceq p$, the only other option is $(p, a) = 1$, as claimed. □

[1] We're keeping the division partial order $\preceq$ notation from last time.

[2] What do you think ℓ stands for?

[3] Why? You should think carefully about this until you come up with an answer. Note that even in calculus class, when talking about infinite series, you never take a sum of an infinite number of numbers. Explain how this can be.

[4] Is, in fact.

[5] As a professor once told me: "A good Lemma is worth its weight in Theorems."

Proposition 7. *Let $p \in \mathcal{P}$ be prime and $a, b \in \mathbb{N}$. If $p \preceq ab$, then $p \preceq a$ or $p \preceq b$.*

Proof. Suppose not, so $p \not\preceq a$ and $p \not\preceq b$. By the previous Lemma, we must have $(p, a) = 1 = (p, b)$. By our construction of the GCD of two numbers from last time,[6] there are integers $x, y, x', y' \in \mathbb{Z}$ such that

$$1 = px + ay \qquad\qquad 1 = px' + by'.$$

We can therefore write

$$1 = (px + ay)(px' + by') = p^2xx' + pbxy' + pax'y + abyy'.$$

Clearly p divides the first three terms of the four-term sum, and by assumption that $p \preceq ab$, p divides the fourth as well. Therefore we conclude[7] that p divides the right hand side, so $p \preceq 1$. This is impossible, so we conclude that our assumption that p does not divide a or b must have been false. □

Corollary 8. *If $p \in \mathcal{P}$ is prime and $a_1, a_2, \ldots, a_n \in \mathbb{N}$ are such that $p \preceq \prod_{i=1}^{n} a_i$, then there is some i, $1 \leq i \leq n$, such that $p \preceq a_i$.*

Proof. We argue by induction. The case that $n = 2$ was the previous Proposition.[8]

Assume the result for some $k \in \mathbb{N}$, and pick $a_1, a_2, \ldots, a_k, a_{k+1} \in \mathbb{N}$ such that $p \preceq \prod_{i=1}^{k+1}$. Set $x = \prod_{i=1}^{k} a_i$, so that $p \preceq x \cdot a_{k+1}$. By the Proposition, we must have $p \preceq x$ or $p \preceq a_{k+1}$. If the former, we're done by the inductive hypothesis; if the latter, we're done by obviousness. □

We're almost ready to prove the Fundamental Theorem, but we need a slight reformulation of induction in order for the theorem to go through.

Axiom (Strong Induction)**.** Suppose that $P(n)$ is a Boolean statement, one for each $n \in \mathbb{N}$. If

- $v(P(0)) = \mathtt{T}$, and
- for any $k \in \mathbb{N}$, the assumption $v(P(i)) = \mathtt{T}$ for all $i < k$ implies $v(P(k)) = \mathtt{T}$,

then $v(P(n)) = \mathtt{T}$ for all $n \in \mathbb{N}$.

Exercise. Show that this formulation of induction is equivalent (in $\mathbb{N}$) to the one we first gave in class.

Proof. (Fundamental Theorem of Arithmetic)

This is actually a unique existence proof: The existence is that the numbers $\ell_p(n)$ can be defined in such a way that the conclusion holds, and the uniqueness is that only one such set of numbers will do.[9]

Existence: We argue by Strong Induction: The case $n = 1$ is solved by setting $\ell_p(1) = 0$ for all $p \in \mathcal{P}$. The case $n = 0$ is outside the purview of the Theorem, so we ignore it.

Fix some $k \in \mathbb{N}$ and assume that for all $i < k$, the numbers $\ell_p(i)$ can be chosen such that $i = \prod_{p \in \mathcal{P}} p^{\ell_p(i)}$. There are two options to consider: Either k is prime, or it is not.[10] If k is prime, $k \in \mathcal{P}$, and we can set

$$\ell_p(k) = \begin{cases} 1 & p = k \\ 0 & p \neq k \end{cases}.$$

It is straightforward to check that this collection of numbers satisfies the conclusion of the Theorem.

[6] Recall: (a, b) is the smallest positive natural number that can be written as an integral linear combination of a and b.
[7] Remind yourself why this is true.
[8] What about $n = 0, 1$?
[9] I.e., $\ell_p(n)$ is *well-defined*.
[10] There are 10 types of people in the world: Those who understand binary, ...

If, however, k is not prime, then by definition there is some $a \in \mathbb{N}$, $1 < a < k$, such that $a \preceq k$. By definition of $\preceq$, this means that there is some other $b \in \mathbb{N}$ such that $ab = k$; as $1 < a$, we conclude that $b < k$. Therefore both a and b are covered by our inductive hypothesis, and we have defined number $\{\ell_p(a)\}_{p\in\mathcal{P}}$ and $\{\ell_p(b)\}_{p\in\mathcal{P}}$ as per the conclusion. Set $\ell_p(k) = \ell_p(a) + \ell_p(b)$, and check that this works. By Strong Induction, this completes the existence proof.

Uniqueness: We want to show that if $n \in \mathbb{N}$, and there are two different sets of number $\{\ell_p(n)\}$ and $\{\ell'_p(n)\}$ such that $n = \prod_{p\in\mathcal{P}} p^{\ell_p(n)} = \prod_{p\in\mathcal{P}} p^{\ell'_p(n)}$, then $\ell_p(n) = \ell'_p(n)$ for all $p \in \mathcal{P}$. Note that this is clear when $n = 1$, as $\ell_p(1) = 0$ for all p is clearly the only possible choice.

Suppose that there is some number n that has two distinct factorizations (i.e., the uniqueness conclusion fails). By the well-ordering of $\mathbb{N}$, there is a smallest such n, and by our observation that 1 has a unique factorization, we must have $1 < n$.

So, by assumption, we have our two sets of natural numbers $\{\ell_p(n)\}$ and $\ell'_p(n)\}$ indexed by $\mathcal{P}$. We know that there is some $q \in \mathcal{P}$ such that $\ell_q(n) \neq 0$.[11] I claim that this forces $\ell'_q(n) = 0$: If not, then $\frac{n}{q} \in \mathbb{N}$,[12] and

$$\ell_p\left(\frac{n}{q}\right) := \begin{cases} \ell_p(n) - 1 & p = q \\ \ell_p(n) & p \neq q \end{cases} \qquad \ell'_p\left(\frac{n}{q}\right) := \begin{cases} \ell'_p(n) - 1 & p = q \\ \ell'_p(n) & p \neq q \end{cases}$$

gives two distinct factorizations for $\frac{n}{q}$.[13] But $\frac{n}{q} < n$, contrary to our assumption that n was minimal with respect to having a nonunique factorization.

But this actually means we're done: If we focus on the $q \in \mathcal{P}$ such that $\ell_q(n) \neq 0$ and $\ell'_q(n) = 0$, then we have (since $q \preceq n$)

$$q \preceq \prod_{\substack{p\in\mathcal{P} \\ \ell'_p(n)\neq 0}} p^{\ell'_p(n)} = p_1^{\ell'_{p_1}(n)} \cdot p_2^{\ell'_{p_2}(n)} \cdot \ldots \cdot p_s^{\ell'_{p_s}(n)}.$$

By the Corollary to our Proposition, this means that $q \preceq p_i^{\ell'_{p_i}(n)}$ for some i, $1 \leq i \leq s$. Writing out $p_i^{\ell'_{p_i}(n)} = \underbrace{p_i \cdot p_i \cdot \ldots \cdot p_i}_{\ell'_{p_i}(n)}$ and applying the Proposition again, this means $q | p_i$. As p_i is prime, this forces $q = p_i$, a contradiction.

□

Final thoughts: We can use this to show the truly fundamental fact that the set of primes $\mathcal{P}$ is infinite.

Theorem 9. *$\mathcal{P}$ is finite.*

Proof. Suppose that $\mathcal{P}$ is finite, say $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$. Then we can define a number

$$q := \left(\prod_{i=1}^{n} p_i\right) + 1.$$

Clearly q is not prime, because it is not equal to p_i for any i. On the other hand, the Fundamental Theorem of Arithmetic says that we can write q as a product of powers of primes; by definition, any prime number p such that $\ell_p(q) \neq 0$ must be one such that $p \preceq q$. But none of the p_i divide q, a contradiction. □

[11] Why?

[12] This is the first time we've used this notation. It is defined to mean: As $q|n$, there is some number m such that $q \cdot m = n$. Exercise: Show that m is unique. We *define* $\frac{n}{q} := m$.

[13] Again, why? Show this using the Well-Ordering Principle.

12. Beginnings of Modular Arithmetic

Just to show that there's more to the universe than $\mathbb{N}$ and $\mathbb{Z}$, let's define an infinite family of algebraic objects, one for each natural number greater than 1:

Definition 10. Let $\mathbb{Z}/n$ denote the set $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Define an addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}/n$ by the rules

$$\overline{a} \oplus \overline{b} : \overline{a + b \mod n} \qquad \overline{a} \odot \overline{b} := \overline{a \cdot b \mod n}.$$

Here, the symbols $+$ and $\cdot$ represent the standard addition and multiplication in $\mathbb{Z}$; the rules state that you take two elements of $\mathbb{Z}/n$, forget about the bar on top, add/multiply as normal, and then reduce the product mod n.

Exercise. Show that $\oplus$ and $\odot$ are both associative, commutative, and have identities. Identify the identities, and show that for $\oplus$, inverses exist, while for $\odot$ they need not. Show that $\odot$ distributes over $\oplus$.

In other words, $\mathbb{Z}/n$ is, like $\mathbb{Z}$, a *commutative ring with identity.*

Example 11. In $\mathbb{Z}/6$, we have

$$\overline{2} \odot \overline{3} = \overline{2 \cdot 3 \mod 6} = \overline{6 \mod 6} = \overline{0},$$

showing that we need not have the product of nonzero of elements of $\mathbb{Z}/n$ is nonzero.

In $\mathbb{Z}/5$, we have

$$\overline{2} \odot \overline{3} = \overline{2 \cdot 3 \mod 5} = \overline{6 \mod 5} = \overline{1},$$

showing that more elements than ± 1 can have multiplicative inverses.

Definition 12. $\overline{a} \in \mathbb{Z}/n$.

- $\overline{a}$ is a *zero divisor* if there is some $\overline{b} \in \mathbb{Z}/n$ such that $\overline{a} \odot \overline{b} = \overline{0}$.
- $\overline{a}$ is a *unit*, or is *invertible*, if there is some $\overline{b} \in \mathbb{Z}/n$ such that $\overline{a} \odot \overline{b} = \overline{1}$.

Exercise. Show that if $\overline{a} \in \mathbb{Z}/n$ is a zero divisor, then $\overline{a}$ is not a unit. Show that if $\overline{a}$ is a unit, then $\overline{a}$ is not a zero divisor. Can there be elements of $\mathbb{Z}/n$ that are neither zero divisors nor units?