Introduction to Abstract Mathematics
Spring 2017

Proving that all naturals (at least 2) are products of primes

What follows is an attempt to carefully establish that every natural number, at least two, is a product of primes. The main goal is to either avoid introducing the mysterious k that occurred in the proof in class, or include it in a more rigorous way.

Remarks:

- For convenience we will say that a single prime number is a product of one prime(s). Not only will this simplify the statement and proof of our result, but it can also be justified by writing
$$p = \prod_{j=1}^{1} p_j,$$
where $p = p_1$. Naturally, this is only a suggestion and can be entirely ignored by the reader if she so desires.
- Mathematicians frequently use the terms "is equal to" and "can be written as" interchangeably. Personally, I tend to prefer the latter.
- Number theorists, such as myself, tend to refer to "prime numbers" as simply "primes." This is, again, another "abuse of terminology" to watch out for.
- Number theorists also like to use the term "divisor" and "factor" interchangeably, since they liteally mean the same thing. So suppose we want to talk about the fact that a given integer n can be written as a product of primes. Each such prime is a divisor, and hence a factor, of n, and so what we really obtain by expressing n as a product of primes is a *prime factorization of* n.

Theorem. *Let $n \geq 2$. Then n has a prime factorization.*

First proof. . By strong induction on n. Since $n = 2$ is prime, it provides its own prime factorization. So now assume that for some $n \geq 2$ we have established that every integer between 2 and n has a prime factorization, and consider $n + 1$. If $n + 1$ is prime, it provides its own prime factorization. If $n + 1$ is composite, then $n + 1 = ab$ for some $a, b \in \{2, 3, \ldots n\}$. In particular, we may apply the inductive hypothesis to both a and b to conclude that they both have prime factorizations. Hence $n + 1 = ab$ does, too. So, in any case, we have shown that if every integer between 2 and n has a prime factorization, then so does $n + 1$. In particular, $2, 3, \ldots n + 1$ all have prime factorizations. By strong induction, every $n \geq 2$ has such a factorization. □

I added the penultimate line of the proof for a specific reason. It's common to present the logic of (this particular) proof by strong induction as follows. To prove $P(n) =$ "n has a prime factorization$''$ for all $n \geq 2$, establish that:
$$P(2) \text{ and } \forall n \geq 2\, (P(2) \wedge P(3) \wedge P(4) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)).$$
We argued in class that this seems to be a perfectly acceptable argument, but it makes it look like strong induction is somehow different than ordinary induction. It's not. Instead, let's let
$$P(n) = \text{“Every integer between 2 and } n \text{ has a prime factorization.''}$$

Then a close look at how I wrote the final line of the first proof shows that what I proved is

$$P(2) \text{ and } \forall n \geq 2\, (P(n) \Rightarrow P(n+1))\,,$$

which certainly qualifies as a "naïve" proof by induction, and clearly implies the result that we're after.

Second proof. By strong induction on n. Since $n = 2$ is prime, it provides its own prime factorization. So now assume that for some $n \geq 2$ we have established that every integer $2 \leq k \leq n$ has a prime factorization, and consider $n + 1$. If $n + 1$ is prime, it provides its own prime factorization. If $n + 1$ is composite, then $n + 1 = ab$ for some a, b satisfying $2 \leq a \leq n$ and $2 \leq b \leq n$. In particular, we may apply the inductive hypothesis to both a and b to conclude that they both have prime factorizations. Hence $n + 1 = ab$ does, too. So, in any case, we have shown that if every integer between 2 and n has a prime factorization, then so does $n + 1$. [In particular, $2, 3, \dots n + 1$ all have prime factorizations.] By strong induction, every $n \geq 2$ has such a factorization. □

The only real difference between this and the preceding proof is the provision of the explicit label k for the integers in $[2, n]$, "every integer $2 \leq k \leq n$" versus the somewhat more open ended "every integer between 2 and n" of the first proof. As mentioned earlier, the sentence in brackets can be safely omitted without altering the logical validity of the argument. Although the mathematical tyro might understandably find the second proof a bit more explicit and easier to understand, I prefer the first simply because it feels a bit simpler and clear cut.