

One problem, three proofs.

Claim: Every natural number greater than one has a prime factor.

(You may try proving this yourself by WOP, PCI, and PMI before reading these proofs if you like.)

1. Proof by WOP.

Let T be the set of natural numbers greater than one that have *no* prime factors.

The claim asserts that T is empty. Suppose for contradiction that T is nonempty; that is, suppose there is some natural number greater than one, with no prime factor. Now T is a nonempty subset of \mathbb{N} , so, by the WOP, T contains some smallest element, n .

Since n is a natural number greater than one, it must be either prime or composite.

Case 1: n is prime. In this case, n is its own prime factor, contradicting the fact that n has no prime factor.

Case 2: n is composite. In this case n has a factor r , with $1 < r < n$. Since n is the smallest member of T and $r < n$, we know that r does not belong to T . Now it must be false that r is a natural number greater than one with no prime factor (by the definition of T), and yet we already know $r > 1$. Thus r has a prime factor, p . So, p is also a prime factor of n , which again contradicts the fact that n has no prime factor.

In either case, we arrive at a contradiction, so T must be empty. That is, every natural number greater than one has a prime factor. QED.

(In this proof T represents the set of counterexamples to the claim. The proof I gave in class was very similar but did not involve T so explicitly.)

2. Proof by PCI.

Let S be the set of all natural numbers n such that either $n = 1$ or n has a prime factor.

We will show that S has the Complete Inductive property; that is, we will show that for any natural number n : if every natural number $m < n$ belongs to S , then n belongs to S . So, let n be a natural number. Suppose all natural numbers $m < n$ belong to S (this is our inductive hypothesis). We have three cases.

Case 1: $n = 1$. In this case, by the definition of S , $n \in S$.

Case 2: n is prime. In this case, n is its own prime factor, so $n \in S$.

Case 3: n is composite. Then n has a factor r , with $1 < r < n$. By our inductive hypothesis, r belongs to S . Since $r \in S$ and $r > 1$, we conclude that r must have a prime factor p . Since $p|r$ and $r|n$, we conclude that $p|n$; thus, p is a prime factor of n .

We have shown that S is a subset of \mathbb{N} with the complete inductive property, so $S = \mathbb{N}$. That is, for any natural number n , either $n = 1$ or n has a prime factor. Thus, every natural number greater than one has a prime factor. QED.

3. Proof by PMI.

(PMI is not ideally suited to this problem, although it can be made to work. It will require a slight hack.)

Let S be the set of natural numbers n such that for any natural number $m < n$, either $m = 1$ or m has a prime factor. (The definition of S from the PCI proof would *not* work here, for a longer reason than I want to get into.)

Base Case: $n = 1$. Note that $1 \in S$, because the statement “for any natural number $m < 1$, either $m = 1$ or m has a prime factor” is vacuously true. (There are no natural numbers $m < 1$.)

Inductive Step: suppose that $n \in S$; that is, suppose that for any natural number $m < n$, either $m = 1$ or m has a prime factor. We are to prove that $n + 1 \in S$, which is to say: for any natural number $m < n + 1$, either $m = 1$ or m has a prime factor. So, we consider an arbitrary $m < n + 1$. Since m is a natural number less than $n + 1$, either $m = n$ or $m < n$. If it happens that $m < n$, then the rest of the claim follows from our inductive hypothesis; thus, we must argue only the case $m = n$. That is, we must show that either $n = 1$ or n has a prime factor. For any natural number n , one of the following occurs: $n = 1$; n is prime; n is composite. Thus we have three cases:

Case 1: $n = 1$. Then $n = 1$ or n has a prime factor.

Case 2: n is prime. Then n is its own prime factor.

Case 3: n is composite. Then n has a factor r , with $1 < r < n$. By our inductive hypothesis, r has a prime factor p . Since $p|r$ and $r|n$, we conclude that $p|n$; thus, p is a prime factor of n .

We have proven that for any natural number $m < n + 1$, either $m = 1$ or m has a prime factor. That is, if $n \in S$, then $n + 1 \in S$. Now $1 \in S$ and S is inductive, so $S = \mathbb{N}$. (If you reread the definition of S , you may see that this does not obviously imply what we were after in the first place.)

Now consider any natural number $k > 1$. Since $k + 1$ is a natural number and $S = \mathbb{N}$, $k + 1 \in S$. That is, every natural number less than $k + 1$ either is 1 or has a prime factor. In particular, $k < k + 1$, so $k = 1$ or k has a prime factor. But $k \neq 1$, so k has a prime factor. Thus, every natural number greater than one has a prime factor. QED.