CSE 311: Foundations of Computing I

Primes Annotated Proofs

Relevant Definitions

Prime DEFINITION

A integer $p > 1$ is *prime* iff the only positive factors of p are 1 and p.

Composite DEFINITION

A integer $p > 1$ is *composite* iff it's not prime. That is, an integer $p > 1$ is composite iff it has a factor other than 1 and p.

Trivial Factor DEFINITION

A *trivial factor* of an integer n is 1 or n. We call it a "trivial factor", because all numbers have these factors.

Fundamental Theorem of Arithmetic THEOREM

Every natural number can be *uniquely* expressed as a product of primes raised to powers.

$\sqrt{n}$ is Fun Root Of n

Prove that if $n \in \mathbb{N}$ is not prime, then it has a non-trivial factor $f \in \mathbb{N}$ where $f \leq \sqrt{n}$.

Proof	Commentary & Scratch Work
Let $n \in \mathbb{N}$ be an arbitrary composite number.	*We're proving a forall statement.*
Then, $n = f_1 f_2$ for non-trivial factors f_1 and f_2, by the definition of composite.	*We want to prove something about n; so, use what we know about n.*
Suppose, for contradiction, that $f_1 > \sqrt{n}$ and $f_2 > \sqrt{n}$.	*We go by contradiction because it's totally unclear* what the factor actually is.
Then, we have $n = f_1 f_2 > (\sqrt{n})(\sqrt{n}) = n$. But $n \not> n$; so, we have a contradiction.	*Our contradiction is that $n > n$ which we see immediately from our assumptions.*
It follows that n has a non-trivial factor f, where $f \geq \sqrt{n}$.	*Conclude the proof.*

Infinitely Many Primes!

Prove that there are infinitely many primes.

N.B. This proof is totally non-obvious. We would not expect you to magically come up with an insight like this without first discussing similar insights.

Proof	Commentary & Scratch Work
Suppose for contradiction that there are finitely many primes.	*We go by contradiction, because primes are hard to deal with, and we have no idea why this is true a priori.*
Since there are finitely many primes, there are n primes for some $n \in \mathbb{N}$. So, we can enumerate the primes as follows: $p_1, p_2, p_3, \ldots, p_n$.	*A direct consequence of the fact that there are finitely many of something is that we can say there are a particular number of them. This allows us to list them out.*
Consider the quantity $N = (p_1 p_2 \cdot p_n) + 1$.	*This is the "magic" step. The general insight is that if there are no more primes, then what is the next number made out of?*
Either N is prime or it is composite. We go by cases.	
Case 1 (N is prime):	
Suppose N is prime. Then, N must be on the list $p_1, p_2, \ldots, p_n$. But $N > p_i$ for any prime p_i. This is a contradiction.	*The idea here is that we already have the largest prime; so, N cannot be it.*
Case 2 (N is composite):	
Suppose N is composite. Then, we know two things: • First, $p_i \mid N$ for some p_i. • Second, $p_i \mid (p_1 p_2 \cdots p_n)$, because p_i is in that product.	*Since we're going by contradiction, the idea is to get as much useful information as possible. Eventually, the contradiction here is going to be "two consecutive numbers do not both have the same prime as a factor".*
Let $P = p_1 p_2 \cdots p_n$.	
Then, by definition of divides, we have $N = kp_i$ and $P = jp_i$. Subtracting the equations, we have $(k-j)p_i = N - P = (P+1) - P = 1$.	*We take our two equations and massage them together.*
So, by definition of divides, $p_i \mid 1$. But this is impossible, because $p_i \geq 2$.	*Going back via definition, we're left with non-sense. It cannot possibly be the case that $\frac{1}{p_i} \in \mathbb{Z}$, because $p_i > 1$.*
So, there is no largest prime. So, there are infinitely many primes.	*Conclude the proof.*