Justin Ventura & Blaine Mason COSC420 LAB1

Question C: justify/prove the fact that you only need to check up to $\sqrt{N}$ in the primality test.

Suppose $N = a \cdot b$ s.t. $a, b \in \mathbb{R}$, $N \in \mathbb{N}$.
(note: this def of N implies it is not prime)

without loss of generality, assume $1 < a \leq b < N$

then take $a < a^2 \leq ab < Na$, note: $N = a \cdot b$

so: $a < a^2 \leq N < a^2 b \rightarrow \sqrt{a} < \boxed{a \leq \sqrt{N}} < a \cdot \sqrt{b}$

same logic: $1 < a \leq b < N \rightarrow b < ab \leq b^2 < Nb$

$\rightarrow \sqrt{b} < \boxed{\sqrt{N} \leq b} < b \cdot \sqrt{a}$

thus, if N is not prime, then two of its factors excluding 1 & N; a, b will be scattered in the range $(1, N)$: a below or equal to $\sqrt{N}$ and b above or at $\sqrt{N}$.

therefore: if N is not prime, you will find at LEAST one factor before you reach $\sqrt{N} + 1$. So reaching $\sqrt{N}$ without a divisor in the algorithm implies that N must be prime.