Lemma TP. Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Proof. Let $a, b, c \in \mathbb{Z}$ be given such that $a|b$ and $b|c$. By definition, $b = ax$ and $c = by$ for some $x, y \in \mathbb{Z}$. Substituting into c,

$$\begin{aligned} c &= (ax)y \\ &= a(xy). \end{aligned}$$

By CPI, $xy = t$ for $t \in \mathbb{Z}$. Thus, $a|c$. $\square$

2.3 Theorem. A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.

Proof. Let a natural number $n > 1$ be given. Suppose n is prime, then $p \nmid n$ for all primes $p \leq \sqrt{n}$. Suppose not. That is, let n be prime, and that there exists a prime $p \leq \sqrt{n}$ such that $p|n$. Since n is prime, by definition on page 29 of our text, we can conclude only $1|n$ and $n|n$. Observe that $p \leq \sqrt{n} < n$. This leads us to conclude $p = 1$, since $p|n$. 1 is not a prime number, this contradicts p being prime. Thus, there does not exist p and $p \nmid n$.

Now we will show if $p \nmid n$ for all primes $p \leq \sqrt{n}$, then n is prime. We will prove by contrapositive. That is, suppose n is composite, there exists a prime $p \leq \sqrt{n}$ such that $p|n$. Since n is composite, let $n = dn'$ for some $d, n' \in \mathbb{Z}$ with $1 < d \leq n'$. Thus,

$$\begin{aligned} d^2 &\leq dn' = n, \\ d^2 &\leq n, \\ d &\leq \sqrt{n}. \end{aligned}$$

Since $d > 1$, by Theorem 2.1, $p|d$. Since $d|n$, by Lemma TP, $p|n$. Thus, n is prime since our contrapositive is true.

Now that we have shown both directions of the biconditional statement to be true, n is prime if and only if $p \nmid n$, for all primes $p \leq \sqrt{n}$. $\square$