Learning Objectives

By the end of this worksheet, you will:

- Prove statements about divisibility and primes.
- Use external facts in a proof.

---

1. Here are two facts about divisibility:

$$\forall n \in \mathbb{N}^+,\ 1 \mid n \ \wedge \ n \mid n \tag{1}$$
$$\forall m, n \in \mathbb{N}^+,\ m \mid n \Rightarrow m \leq n \tag{2}$$

Write the contrapositive of the second fact.

Make sure these facts (including the contrapositive of the second one) seem correct to you, then for the rest of the worksheet you may assume/use these facts.

For each fact, state when we are allowed to use it, and when we would want to use it.

After finishing the rest of the worksheet try proving the second fact.
Hint: "solve" for the value of a witness to the existential hypothesis.

2. Consider the two propositional formulas $f = (p \wedge q) \vee (r \wedge s)$ and $g = (p \vee r) \wedge (q \vee s)$.

   Imagine a direct proof of a statement of the form $f \Rightarrow g$. Could you prove it without knowing p, q, r, and s, and what would the proof look like?

   Now, consider a statement of the form $g \Rightarrow f$. Does that depend on p, q, r, and s? In other words, does $g \not\Rightarrow f$?

3. Recall that for each $n \in \mathbb{N}^+$ we define $Prime(n)$ as: $n > 1 \wedge \forall d \in \mathbb{N}^+,\ d \mid n \Rightarrow d = 1 \vee d = n$. **[Corrected by adding missing "$n > 1$".]**

   Consider the following facts:

$$\forall n \in \mathbb{N}^+, Prime(n) \Rightarrow \forall a, b \in \mathbb{N}^+, n = a \cdot b \Rightarrow (a = 1 \wedge b = n) \vee (a = n \wedge b = 1) \tag{3}$$

$$\forall n \in \mathbb{N}^+, Prime(n) \Rightarrow \forall a, b \in \mathbb{N}^+, n = a \cdot b \Rightarrow (a = 1 \vee a = n) \wedge (b = 1 \vee b = n) \tag{4}$$

   Make sure these facts seem correct to you, then for the rest of the worksheet you may assume/use these facts.

   How are we most likely to use one of these facts directly (as opposed to in the various contrapositive forms). Then write (either) one of them as an equivalent statement in the form $\forall n, a, b \in \mathbb{N}^+, (\cdots) \Rightarrow (\cdots)$, without using any universals nor implications inside the $(\cdots)$s.

   State which one is *stronger*, due to it entailing the other *regardless* of the meanings of *Prime*, $\cdot$, and $=$.

   After finishing the rest of the worksheet try proving the stronger fact, and then prove the weaker one from it.

4. Prove the statement we discussed in lecture:

$$\forall n \in \mathbb{N}^+,\ \big(n > 1 \land \forall a, b \in \mathbb{N}^+,\ n \mid ab \Rightarrow n \mid a \lor n \mid b\big) \Rightarrow Prime(n)$$