Learning Objectives

By the end of this worksheet, you will:

- Prove statements about primes and greatest common divisors.
- Understand and use external claims in a proof.

Here are some facts about divisibility, primes, and greatest common divisors that you'll use for this worksheet (you do not need to prove them before using them). Read them carefully and make sure you understand what each one is saying before moving onto the first question. You may find it helpful to translate them into English on a separate sheet of paper for extra practice.

\[
\forall x \in \mathbb{N}, x \mid x \quad \text{(Claim 1)}
\]

\[
\forall x, y \in \mathbb{N}, y \geq 1 \land x \mid y \Rightarrow 1 \leq x \land x \leq y \quad \text{(Claim 2)}
\]

\[
\forall n, p \in \mathbb{N}, \text{Prime}(p) \land p \nmid n \Rightarrow \gcd(p, n) = 1 \quad \text{(Claim 3)}
\]

\[
\forall n, m \in \mathbb{Z}^+, \gcd(n, m) \geq 1 \quad \text{(Claim 4)}
\]

\[
\forall n, m, r, s \in \mathbb{Z}, \gcd(n, m) \mid (rn + sm) \quad \text{(Claim 5)}
\]

\[
\forall n, m \in \mathbb{N}, \exists r, s \in \mathbb{Z}, rn + sm = \gcd(n, m) \quad \text{(Claim 6)}
\]

Here is a reminder of two definitions from the Week 4 Hour 2 Session (Worksheet 6):

**Definition 1** (common divisor, greatest common divisor). Let \(x, y, d \in \mathbb{Z}\). We say that \(d\) is a common divisor of \(x\) and \(y\) if and only if \(d\) divides \(x\) and \(d\) divides \(y\). We say that \(d\) is the greatest common divisor of \(x\) and \(y\) if and only if it is the maximum common divisor of \(x\) and \(y\), and in this case write \(d = \gcd(x, y)\).

1. Recall the statement we considered and (mostly) proved in lecture last Thursday:

\[
\forall n \in \mathbb{N}, \neg \text{Prime}(n) \Rightarrow \left( n \leq 1 \lor (\exists a, b \in \mathbb{N}, n \nmid a \land n \nmid b \land n \mid ab) \right)
\]

In this exercise, you will work with the equivalent statement:

\[
\forall n \in \mathbb{N}, \neg \text{Prime}(n) \land n > 1 \Rightarrow (\exists a, b \in \mathbb{N}, n \nmid a \land n \nmid b \land n \mid ab)
\]

You should convince yourself that the two statements are equivalent!

We have provided a proof header for you below. Read through it carefully to make sure you understand it, and then using Claims 1 and 2, complete the proof. Whenever you use one of these claims, clearly state which claim you are using.

**Hint:** you may want to use the contrapositive of the implication in (Claim 2) as well.

**Proof.** Let \(n \in \mathbb{N}\). Assume that \(n\) is not prime, and that \(n > 1\). Then (from the definition of prime), there exists \(d \in \mathbb{N}\), \(d \nmid n \land d \neq 1 \land d \neq n\). Expanding the definition of the divides predicate, this means that there also exists \(k \in \mathbb{N}\) such that \(n = dk\). Let \(a = d\) and \(b = k\). We want to prove that \(n \nmid a, n \nmid b, \text{ and } n \mid ab\).

Since we’re running out of space, turn the page over and complete the proof.

---

\(^1\) For Claims 5 and 6, we define \(\gcd(0, 0) = 0\) so that these two claims hold for all pairs of natural numbers.
Proof. Let $n \in \mathbb{N}$. Assume that $n$ is not prime, and that $n > 1$. Then (from the definition of prime), there exists $d \in \mathbb{N}$, $d \mid n$ and $d \neq 1, d \neq n$. Expanding the definition of the divides predicate, this means that there also exists $k \in \mathbb{N}$ such that $n = dk$. Let $a = d$ and $b = k$. We want to prove that $n \nmid a$, $n \nmid b$, and $n \mid ab$.

2. Our next lecture example was the contrapositive form of the converse of the first statement in Question 1:

$$\forall n \in \mathbb{N}, \text{Prime}(n) \Rightarrow \left( n > 1 \land (\forall a, b \in \mathbb{N}, \ n \nmid a \land n \nmid b \Rightarrow n \nmid ab) \right)$$

We proved the statement in lecture using two claims, which you’ll now prove using the external facts from the previous page. Whenever you use a statement from the previous page, clearly state which one you are using.
(a) \forall n, m \in \mathbb{N}, \text{Prime}(n) \land n \nmid m \Rightarrow (\exists r, s \in \mathbb{Z}, rn + sm = 1).

(b) \forall n, m \in \mathbb{N}, \text{Prime}(n) \land (\exists r, s \in \mathbb{Z}, rn + sm = 1) \Rightarrow n \nmid m.
3. *Extra.* For extra practice, try proving Claims 1-5\(^2\). They can all be proven using the definitions of divisibility, prime, and gcd. Try to use as few external facts as possible, and if you use any, prove them as well!

---

\(^2\) Claim 6 is quite a bit harder to prove, so don’t worry about proving it here.