Learning Objectives

By the end of this worksheet, you will:

- Prove and 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 this now). 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.[1]

$$\forall x \in \mathbb{N},\ x \mid x \qquad \text{(Claim 1)}$$
$$\forall x, y \in \mathbb{N},\ y \geq 1 \land x \mid y \Rightarrow 1 \leq x \land x \leq y \qquad \text{(Claim 2)}$$
$$\forall n, p \in \mathbb{N},\ Prime(p) \land p \nmid n \Rightarrow \gcd(p, n) = 1 \qquad \text{(Claim 3)}$$
$$\forall n, m \in \mathbb{Z}^+,\ \gcd(n, m) \geq 1 \qquad \text{(Claim 4)}$$
$$\forall n, m, \in \mathbb{N},\ \forall r, s \in \mathbb{Z},\ \gcd(n, m) \mid (rn + sm) \qquad \text{(Claim 5)}$$
$$\forall n, m \in \mathbb{N},\ \exists r, s \in \mathbb{Z},\ rn + sm = \gcd(n, m) \qquad \text{(Claim 6)}$$

1. Recall the first statement we proved this week:

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

We have provided a proof header for you already. Read through it carefully and 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 (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 $d \in \mathbb{N},\ d \mid n \land d \neq 1 \land d \neq n$. 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 $n \nmid a$, $n \nmid b$, and $n \mid ab$.

□

[1] For Claims 5 and 6, we *define* $\gcd(0, 0) = 0$ so that these two claims hold for all pairs of natural numbers.

2. Our second example was the converse form of the first statement:

$$\forall n \in \mathbb{N},\ Prime(n) \lor n \leq 1 \Rightarrow \big(\forall a, b \in \mathbb{N},\ n \nmid a \land n \nmid b \Rightarrow n \nmid ab\big)$$

We proved it 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) $\forall n, m \in \mathbb{N},\ Prime(n) \land n \nmid m \Rightarrow \big(\exists r, s \in \mathbb{Z},\ rn + sm = 1\big)$.

(b) $\forall n, m \in \mathbb{N},\ Prime(n) \land \big(\exists r, s \in \mathbb{Z},\ rn + sm = 1\big) \Rightarrow n \nmid m$.

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.