Learning Objectives

By the end of this worksheet, you will:

- Prove statements about primes and greatest common divisors.
- Use external facts in a proof.

Here is a reminder of two definitions from 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 when d divides x and d divides y. When x and y are not both 0, we say that d is the **greatest common divisor (gcd)** of x and y when it is the maximum common divisor of x and y. We also define the greatest common divisor of 0 and 0 to be equal to 0 (as a special case).

We also define the function $\gcd : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ to be the function that takes two integers and returns their greatest common divisor.

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 for extra practice.[1]

$$\forall x \in \mathbb{Z},\ x \mid x \tag{Fact 1}$$

$$\forall x, y \in \mathbb{N},\ y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \tag{Fact 2}$$

$$\forall n, p \in \mathbb{Z},\ Prime(p) \wedge p \nmid n \Rightarrow \gcd(p, n) = 1 \tag{Fact 3}$$

$$\forall n, m \in \mathbb{N},\ n \neq 0 \vee m \neq 0 \Rightarrow \gcd(n, m) \geq 1 \tag{Fact 4}$$

$$\forall n, m, \in \mathbb{N},\ \forall r, s \in \mathbb{Z},\ \ \gcd(n, m) \mid (rn + sm) \tag{Fact 5}$$

$$\forall n, m \in \mathbb{N},\ \exists r, s \in \mathbb{Z},\ rn + sm = \gcd(n, m) \tag{Fact 6}$$

[1] Facts 4, 5, and 6 rely on defining $\gcd(0, 0) = 0$ so that the statements hold for all pairs of natural numbers.

1. Recall the first statement we considered in lecture this week:

$$\forall n \in \mathbb{N},\ \neg Prime(n) \Rightarrow \Big(n \leq 1 \vee \big(\exists a, b \in \mathbb{N},\ n \nmid a \wedge n \nmid b \wedge n \mid ab\big)\Big)$$

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, i.e., that $n \leq 1$ or there exists a $d \in \mathbb{N}$ such that $d \mid n$, $d \neq 1$, and $d \neq n$ (this is the expanded definition of $\neg Prime(n)$. We want to prove that $n \leq 1$ or that there exist $a, b \in \mathbb{N}$ such that $n \nmid a$, $n \nmid b$, and $n \mid ab$.

Since our assumption is an OR, we will divide our proof into two cases (based on which part we assume to be true).

Case 1: assume that $n \leq 1$.

Case 2: assume there exists $d \in \mathbb{N}$ where $d \mid n \wedge d \neq 1 \wedge d \neq n$. Expanding the definition of divisibility, this means that there also exists $k \in \mathbb{N}$ such that $n = dk$.[2] Also, because we handled the case of $n \leq 1$ in “Case 1” above, we can assume in this case that $n > 1$.

Let $a = d$ and $b = k$. We want to prove that $n \nmid a$, $n \nmid b$, and $n \mid ab$.

□

[2] **Updated Jan 29**: as noted in the Course Notes Errata, the correct domain of k from the definition of divisibility is $k \in \mathbb{Z}$. We need an extra sentence to justify why $k \geq 0$, using the fact that $n, d \in \mathbb{N}$.

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

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

We proved the statement in lecture using two facts, 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 Facts 1-5.[3] 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!

[3] Fact 6 is quite a bit harder to prove, so don't worry about proving it here.