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]

$$\forall x \in \mathbb{Z},\ x \mid x \tag{Fact 1}$$
$$\forall x, y \in \mathbb{N},\ y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \tag{Fact 2}$$
$$\forall n, p \in \mathbb{Z},\ \mathit{Prime}(p) \wedge p \nmid n \Rightarrow \gcd(p, n) = 1 \tag{Fact 3}$$
$$\forall n, m \in \mathbb{N},\ n \neq 0 \vee m \neq 0 \Rightarrow \gcd(n, m) \geq 1 \tag{Fact 4}$$
$$\forall n, m, \in \mathbb{N},\ \forall r, s \in \mathbb{Z},\ \gcd(n, m) \mid (rn + sm) \tag{Fact 5}$$
$$\forall n, m \in \mathbb{N},\ \exists r, s \in \mathbb{Z},\ rn + sm = \gcd(n, m) \tag{Fact 6}$$

[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 Facts 1 and 2, complete the proof. Whenever you use one of these facts, clearly state which one you are using.

Hint: you may want to use the contrapositive of the implication in (Fact 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 $n \leq 1$.

Solution

In this case, we've assumed that $n \leq 1$, which is exactly the first part of the OR we wanted to prove.

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 $k \in \mathbb{Z}$ such that $n = dk$. Because $n, d \in \mathbb{N}$, we conclude that $k \in \mathbb{N}$ as well. 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 $n \mid ab$.

Solution

Part 1: proving $n \nmid a$ and $n \nmid b$.
By our choices of a and b, we know that $a \mid n$ and $b \mid n$. By Fact 2 and the assumption $n > 1$, this means that $1 \leq a \leq n$ and $1 \leq b \leq n$. Since we set $a = d$ and we assumed $d \neq n$, we can conclude that $a < n$. And since $a \neq 1$, we can conclude $b \neq n$, and so $b < n$.

The contrapositive of Fact 2 is $\forall x, y \in \mathbb{N},\ x < 1 \vee y < x \Rightarrow x \nmid y \vee y = 0$. Applying this to the deductions $a < n$ (substituting $y = a$ and $x = n$), we can conclude that $n \nmid a \vee a = 0$. Since we have already deduced that $a \geq 1$, we know $a = 0$ is *False*, and so $n \nmid a$.

Applying the contrapositive of Fact 2 to the deductions $b < n$, we can conclude that $n \nmid b \vee b = 0$. Since we have already deduced that $b \geq 1$, we know $b = 0$ is *False*, and so $n \nmid b$.

Part 2: proving $n \mid ab$.
We also know $ab = dk = n$. By Fact 1, we can conclude that $n \mid ab$.

□

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

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

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

Solution

Proof. Let $n, m \in \mathbb{N}$. Assume that n is prime and that $n \nmid m$. We want to prove there exist $r, s \in \mathbb{Z},\ rn + sm = 1$.

By Fact 3 and our two assumptions, we know that $\gcd(n, m) = 1$. And then using Fact 6, there exist $r, s \in \mathbb{Z}$ such that $rn + sm = \gcd(n, m) = 1$. □

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

Solution

Proof. Let $n, m \in \mathbb{N}$. Assume that n is prime, and that there exist $r, s \in \mathbb{Z}$ such that $rn + sm = 1$.

By Fact 5, we know that $\gcd(n, m) \mid (rn + sm)$, i.e., $\gcd(n, m) \mid 1$. Then using Fact 2 (substituting $x = \gcd(n, m)$ and $y = 1$), we know that $1 \leq \gcd(n, m) \leq 1$, and therefore $\gcd(n, m) = 1$.

Since n is prime, its only positive divisors are 1 and itself (by the definition of *prime*). Since $\gcd(n, m) = 1$ and $n > 1$ (by the definition of *prime* again), n is *not* a common divisor of n and m. Finally, since Fact 1 tells us that $n \mid n$, if we know that n is not a common divisor of n and m, it must be that $n \nmid m$. □

3. *Extra.* For extra practice, try proving Facts 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]Fact 6 is quite a bit harder to prove, so don't worry about proving it here.