Learning Objectives

By the end of this worksheet, you will:

- Understand and use the definition of greatest common divisor in statements and proofs.
- Write proofs and disproofs using the proof-by-cases and contrapositive (indrect) proof techniques.

---

1. **Greatest common divisor.** In this question, you'll explore a new definition which is fundamental in number theory: the greatest common divisor between two numbers.

   (a) As a warmup, we are going to first consider how to express the idea of the "greatest" or "maximum" number that satisfies some predicate. Suppose we have a predicate $P : \mathbb{N} \to \{\text{True}, \text{False}\}$. Express in predicate logic the statement "123 is the maximum natural number that satisfies P."
   Hint: Think about trying to complete the sentence "every number that satisfies P is..."

   Solution

   $P(123) \wedge \big(\forall y \in \mathbb{N},\ P(y) \Rightarrow y \leq 123\big)$

   (b) Now consider the following two definitions.

   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 $d = \gcd(x, y)$.

   In the space below, write symbolic formulas to express these predicates. (You can use $IsCD$ in the definition of $IsGCD$.)

   $IsCD(x, y, d)$: "d is a common divisor of x and y," where $x, y, d \in \mathbb{Z}$
   $IsGCD(x, y, d)$: "d is the greatest common divisor of x and y," where $x, y, d \in \mathbb{Z}$

   Solution

   $$IsCD(x, y, d) : \big(\exists k_1 \in \mathbb{Z},\ x = k_1 d\big) \wedge \big(\exists k_2 \in \mathbb{Z},\ y = k_2 d\big)$$
   $$IsGCD(x, y, d) : IsCD(x, y, d) \wedge \big(\forall d_1 \in \mathbb{Z},\ IsCD(x, y, d_1) \Rightarrow d_1 \leq d\big)$$

   Note: for $IsCD$, you can also pull the quantifiers all the way to the left: $\exists k_1 \in \mathbb{Z},\ \exists k_2 \in \mathbb{Z},\ x = k_1 d \wedge y = k_2 d$.

   (c) Using the definition of divisibility and gcd, determine how to complete the following statement, and then prove it. (Note: be very careful about what you're proving, and make sure you give explicit proofs of divisibility here!)

   $$\forall x \in \mathbb{Z}^+,\ \gcd(x, 0) = \_\_\_\_\_$$

   You can use the fact in your proof that for all $n \in \mathbb{Z}^+$ and $d \in \mathbb{Z}$, if d divides n then $d \leq n$.

   Solution

   The full statement we'll prove is

   $$\forall x \in \mathbb{Z}^+,\ \gcd(x, 0) = x$$

   Discussion. We want to prove that $\gcd(x, 0) = x$, which really consists of proving two things:

   - x is a common divisor of x and 0
   - Every common divisor of x and 0 is $\leq x$.

We should be able to do the first part using the definition of divisibility; for the second part, we'll use the fact given in the question.

Proof. Let $x \in \mathbb{N}$. Our proof will be divided into three parts.

Part 1: proving that $x \mid x$.
Let $k_1 = 1$. Then $x = k_1 x$, and so $x \mid x$.

Part 2: proving that $x \mid 0$.
Let $k_2 = 0$. Then $0 = k_2 x$, and so $x \mid 0$.

Part 3: proving that every common divisor of x and 0 is $\leq x$.
Let $d \in \mathbb{Z}$, and assume that d divides both x and 0. Then because $d \mid x$, we know that $d \leq x$. □

(d) Here is one of the most famous and useful properties of the greatest common divisor. We probably won't have time to prove this statement in the course, but we'll certainly use it!

For every pair of integers a and b, $\gcd(a, b)$ is the *smallest positive integer* that can be written in the form $pa + qb$, where p and q are integers.[1]

In the space below, translate the above statement into predicate logic. Use the notation $\mathbb{Z}^+$ to denote the set of positive integers. You may define helper predicates to help simplify your formula.

Solution

Let's define the following helper predicate:*

$$LinComb(a, b, c) : \text{“}\exists p, q \in \mathbb{Z},\ c = pa + qb,\text{”} \text{ where } a, b \in \mathbb{Z}, \text{ and } c \in \mathbb{Z}^+.$$

Then we can express the above statement as:

$$\forall a, b \in \mathbb{Z},\ LinComb(a, b, \gcd(a, b)) \wedge \big(\forall d \in \mathbb{Z}^+, LinComb(a, b, d) \Rightarrow d \geq \gcd(a, b)\big)$$

*We call expressions of the form $pa + qb$ a *linear combination* of a and b.

2. **Proof by cases.** Often when proving a universally-quantified statement, the same argument in a proof does not actually apply to all cases. Consider the following (true) statement:

For every integer n, $n^2 - 3n$ is even.

Such statements are usually easier to prove by dividing the domain into different parts, and giving a different argument for each part separately. We call such a proof a **proof by cases**, where the term "case" refers to one of the different parts of the domain that are considered.

In this question, we will use the fact that every integer is either even or odd, and so divide up our proof into two cases. Learn how a proof by cases works by completing the following proof.

Proof. Let $n \in \mathbb{Z}$. We will divide this proof into two cases: when n is even, and when n is odd.

Case 1: *assume* that n is even, i.e., $\exists k \in \mathbb{Z},\ n = 2k$.

[**TODO**: prove that $n^2 - 3n$ is even, assuming that n is even.]

Solution

This can be proved using a simple calculation. Letting $k_1 = 2k^2 - 3k$, we have:

[1] For example, $\gcd(6, 22) = 2$, and $2 = 7 \cdot 6 + (-2) \cdot 22$.

$$\begin{aligned} n^2 - 3n &= (2k)^2 - 3(2k) \\ &= 4k^2 - 6k \\ &= 2(2k^2 - 3k) \\ &= 2k_1 \end{aligned}$$

Case 2: *assume* that n is odd, i.e., $\exists k \in \mathbb{Z},\ n = 2k - 1$.

[**TODO**: prove that $n^2 - 3n$ is even, assuming that n is odd.]

Solution

Left as an exercise; similar to the previous case.

□

3. **An indirect (contrapositive) proof.** We have seen in lecture that sometimes the contrapositive form of an implication can often be easier to work with when writing a proof. Let's work on a slightly tougher example.

$$\forall a, b \in \mathbb{N},\ 1 < \gcd(a, b) \wedge \gcd(a, b) < b \Rightarrow \neg Prime(b).$$

(a) Write the contrapositive form of the above statement.

Solution

$$\forall a, b \in \mathbb{N},\ Prime(b) \Rightarrow \gcd(a, b) \leq 1 \vee \gcd(a, b) \geq b$$

(b) Prove the above statement. Use two cases: when $b \mid a$, and when $b \nmid a$.
Note: to prove a formula of the form $p \vee q$, you only need to prove that p is true, or that q is true. And since you have two cases, which one you prove to be true can be different for each case!

Solution

Proof. Let $a, b \in \mathbb{N}$ and assume that b is prime. We'll divide this proof into two cases.
Case 1: assume $b \mid a$.
In this case, $\gcd(a, b) = b$, since every divisor of b is $\leq b$. Then $\gcd(a, b) \geq b$.
Case 2: assume $b \nmid a$.
In this case, $\gcd(a, b) = 1$, since the only other positive divisor of b is 1, and $1 \mid a$. Then $\gcd(a, b) \leq 1$. □