

Least greatest proofs

For a set of numbers X , how do you formalize “there is a greatest X ” or “there is a least X ”?

Prove or disprove: There is a least prime number.

Prove or disprove: There is a greatest integer.

Approach 1, De Morgan’s and universal generalization:

Approach 2, proof by contradiction:

Extra examples: Prove or disprove that \mathbb{N} , \mathbb{Q} each have a least and a greatest element.

Gcd definition

Definition: Greatest common divisor Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $\gcd(a, b)$.

Gcd examples

Why do we restrict to the situation where a and b are not both zero?

Calculate $\gcd(10, 15)$

Calculate $\gcd(10, 20)$

Gcd basic claims

Claim: For any integers a, b (not both zero), $\gcd(a, b) \geq 1$.

Proof: *Show that 1 is a common factor of any two integers, so since the gcd is the greatest common factor it is greater than or equal to any common factor.*

Claim: For any positive integers a, b , $\gcd(a, b) \leq a$ and $\gcd(a, b) \leq b$.

Proof *Using the definition of gcd and the fact that factors of a positive integer are less than or equal to that integer.*

Claim: For any positive integers a, b , if a divides b then $\gcd(a, b) = a$.

Proof *Using previous claim and definition of gcd.*

Claim: For any positive integers a, b, c , if there is some integer q such that $a = bq + c$,

$$\gcd(a, b) = \gcd(b, c)$$

Proof *Prove that any common divisor of a, b divides c and that any common divisor of b, c divides a .*

Gcd lemma relatively prime

Lemma: For any integers p, q (not both zero), $\gcd\left(\frac{p}{\gcd(p, q)}, \frac{q}{\gcd(p, q)}\right) = 1$. In other words, can reduce to relatively prime integers by dividing by gcd.

Proof:

Let x be arbitrary positive integer and assume that x is a factor of each of $\frac{p}{\gcd(p, q)}$ and $\frac{q}{\gcd(p, q)}$. This gives integers α, β such that

$$\alpha x = \frac{p}{\gcd(p, q)} \qquad \beta x = \frac{q}{\gcd(p, q)}$$

Multiplying both sides by the denominator in the RHS:

$$\alpha x \cdot \gcd(p, q) = p \qquad \beta x \cdot \gcd(p, q) = q$$

In other words, $x \cdot \gcd(p, q)$ is a common divisor of p, q . By definition of \gcd , this means

$$x \cdot \gcd(p, q) \leq \gcd(p, q)$$

and since $\gcd(p, q)$ is positive, this means, $x \leq 1$.

Definitions

| Term | Notation | Example(s) | We say in English ... |
|---------------------------|---|------------|---|
| sequence | x_1, \dots, x_n | | A sequence x_1 to x_n |
| summation | $\sum_{i=1}^n x_i$ or $\sum_{i=1}^n x_i$ | | The sum of the terms of the sequence x_1 to x_n |
| all reals | \mathbb{R} | | The (set of all) real numbers (numbers on the number line) |
| all integers | \mathbb{Z} | | The (set of all) integers (whole numbers including negatives, zero, and positives) |
| all positive integers | \mathbb{Z}^+ | | The (set of all) strictly positive integers |
| all natural numbers | \mathbb{N} | | The (set of all) natural numbers. Note: we use the convention that 0 is a natural number. |
| piecewise rule definition | $f(x) = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$ | | Define f of x to be x when x is nonnegative and to be $-x$ when x is negative |
| function application | $f(7)$ $f(z)$ $f(g(z))$ | | f of 7 or f applied to 7 or the image of 7 under f f of z or f applied to z or the image of z under f f of g of z or f applied to the result of g applied to z |
| absolute value | $ -3 $ | | The absolute value of -3 |
| square root | $\sqrt{9}$ | | The non-negative square root of 9 |

Defining sets

To define sets:

To define a set using **roster method**, explicitly list its elements. That is, start with $\{$ then list elements of the set separated by commas and close with $\}$.

To define a set using **set builder definition**, either form “The set of all x from the universe U such that x is ...” by writing

$$\{x \in U \mid \dots x \dots\}$$

or form “the collection of all outputs of some operation when the input ranges over the universe U ” by writing

$$\{\dots x \dots \mid x \in U\}$$

We use the symbol \in as “is an element of” to indicate membership in a set.

Example sets: For each of the following, identify whether it’s defined using the roster method or set builder notation and give an example element.

$$\{-1, 1\}$$

$$\{0, 0\}$$

$$\{-1, 0, 1\}$$

$$\{(x, x, x) \mid x \in \{-1, 0, 1\}\}$$

$$\{\}$$

$$\{x \in \mathbb{Z} \mid x \geq 0\}$$

$$\{x \in \mathbb{Z} \mid x > 0\}$$

$$\{\text{A, C, U, G}\}$$

$$\{\text{AUG, UAG, UGA, UAA}\}$$