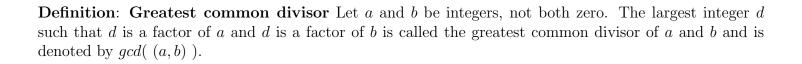
ECONO FICONOS PICON	Least	greatest	proofs
---------------------	-------	----------	--------

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



## 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

<b>Claim</b> : For any integers $a, b$ (not both zero), $gcd((a, b)) \ge 1$ .
---

**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 Pr	ove that	t ann co	nm m on	divisor	of a h	dividee	c and	that and	ı commo	n diviso	r of $h$	divides a	,
1100117	ove mai	any co	mmon	<i>aivi</i> sor	$o_j a, o$	aiviaes	c ana	inai ang	, commo	n aiviso	<i>r 0, 0, c</i>	aiviaes a	

#### Gcd lemma relatively prime

**Lemma**: For any integers p,q (not both zero),  $\gcd\left(\left(\frac{p}{\gcd((p,q))},\frac{q}{\gcd((p,q))}\right)\right)=1$ . 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  $\alpha$ ,  $\beta$  such that

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

Multiplying both sides by the denominator in the RHS:

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

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

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

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

# Definitions

Term	Notation Example(s)	We say in English
sequence	$x_1,\ldots,x_n$	A sequence $x_1$ to $x_n$
summation	$x_1, \dots, x_n$ $\sum_{i=1}^n x_i \text{ or } \sum_{i=1}^n x_i$	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	N	The (set of all) natural numbers. <b>Note</b> : we use the convention that 0 is a natural number.
piecewise rule definition	$f(x) = \begin{cases} x & \text{if } x \ge 0 \\ -x & \text{if } x < 0 \end{cases}$	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 square root	$\begin{array}{c}  -3  \\ \sqrt{9} \end{array}$	The absolute value of $-3$ 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

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

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

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

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.