Mar 23 Slides

Elizabeth Orrico

Agenda

Review: Fundamental Theorem of Arithmetic

Proof by Contradiction Template

Example 1: Irrationals

Example 2:

Intro to Integers

What’s a factor?

a is a factor of ***b*** iff b can be evenly divided by a,

That is, for some integer ***k***

$$\boldsymbol{ak = b}$$

Let’s list the factors of 4!

What’s a factor?

a is a factor of ***b*** iff b can be evenly divided by a,

That is, for some integer ***k***

$$ak = b$$

Let’s list the factors of 4!

1, 2, 4, -4, -2, -1

What’s a factor?

a is a factor of ***b*** iff b can be evenly divided by a,

That is, for some integer ***k***

$$ak = b$$

From this point forward, we will only be referring to the positive integers though.

What’s a prime

A prime is a number greater than 1 that is divisible only by 1 and itself.

Is 2 a prime number?

“Fundamental theorem of Arithmetic”

Aka Unique Factorization thm

“For all natural numbers, there exists a factorization of n such that all factors are prime and the factorization is unique.”

“Fundamental theorem of Arithmetic”

Aka Unique Factorization thm

For all natural numbers, there exists a factorization of n such that al factors are prime and the factorization is unique.

60 = 2*2*3*5

^The one and only way of expressing 60 as a set of prime factors

“Prime factorization” -> multiplicity of factor 2 is 2 (of 5 is 1)

“Fundamental theorem of Arithmetic”

Aka Unique Factorization thm

For all natural numbers, there exists a factorization of n such that al factors are prime and the factorization is unique.

60 = 2^2 *5*3

What is the GCD of 84?

Greatest Common Divisor

A **common divisor** of a and b is a number that divides them both.

The **greatest common divisor** of a and b is the biggest number that divides them both.

gcd(60, 8) = ???

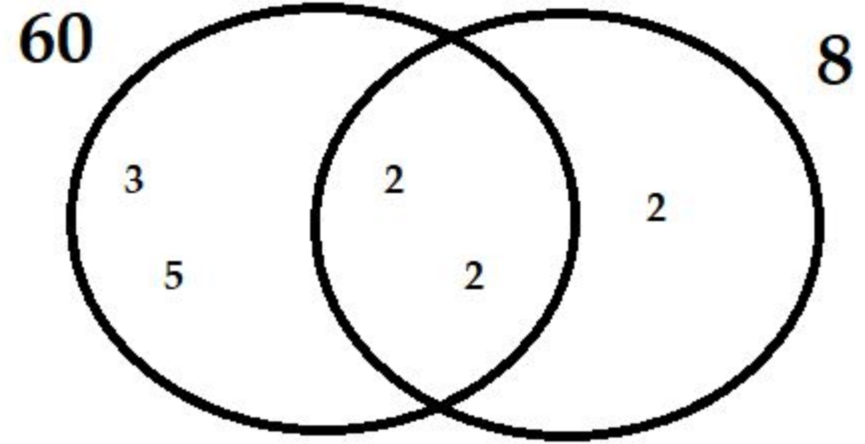
Greatest Common Divisor

A **common divisor** of a and b is a number that divides them both.

The **greatest common divisor** of a and b is the biggest number that divides them both.

gcd(60, 8) = 4

“intersect”



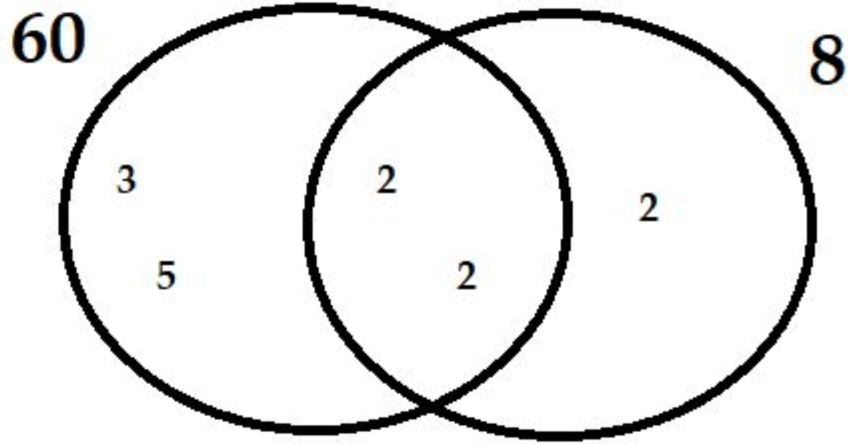
Greatest Common Divisor

A **common divisor** of a and b is a number that divides them both.

The **greatest common divisor** of a and b is the biggest number that divides them both.

gcd(60, 8) = 4

What is gcd(90, 84) = ?



Relatively Prime

Two positive integers greater than 1 are **relatively prime** iff gcd(x, y) = 1

What is number theory?

“Mathematics is the queen of the sciences…..”

~Carl Friedrich Gauss

What is number theory?

“Mathematics is the queen of the sciences…..”

“And **number theory** is the queen of mathematics”

~Carl Friedrich Gauss

What is number theory?

“Mathematics is the queen of the sciences…..”

“And **number theory** is the queen of mathematics”

~Carl Friedrich Gauss

[Number theorists] may be justified in rejoicing that there is one science, at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

~G. H. Hardy

What is number theory?

“Mathematics is the queen of the sciences…..”

“And **number theory** is the queen of mathematics”

~Carl Friedrich Gauss

[Number theorists] may be justified in rejoicing that there is one science, at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

~G. H. Hardy

What is number theory?

Number theory is the study of ***integers.***

Seems simple, but a rich area for questions we can ask easily but don’t know the answer to!

What is number theory?

Number theory is the study of ***integers.***

Seems simple, but a rich area for questions we can ask easily but don't know the answer to!

Goldbach's conjecture: Every even integer greater than 2 is the sum of two primes.

What is number theory?

Number theory is the study of ***integers.***

Seems simple, but a rich area for questions we can ask easily but don't know the answer to!

Goldbach's conjecture: Every even integer greater than 2 is the sum of two primes.

Collatz conjecture: Start with any positive integer n. Then, if the number is even, divide by 2. If it's odd, multiply by 3 and add 1. Repeat. The conjecture is that no matter what value of n, the sequence will always reach 1.

Proof by Contradiction

Proof by contradiction

Theorem: A is true.

We proceed by contradiction.

Assume **Not A** to prove this”

...

Not A proves FALSE

Therein lies the contradiction.

Therefore

A is true.

Often how we prove something is impossible in computing

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Assume ½ IS elem

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Assume ½ IS elem

Means $\exists x \in \mathbb{N}$. s.t $\frac{1}{2} = x$

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Assume ½ IS elem

Means $\exists x \in \mathbb{N}$. s.t $\frac{1}{2} = x$

$1 = 2x$

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Assume ½ IS elem

Means $\exists x \in \mathbb{N}$. s.t $\frac{1}{2} = x$

$1 = 2x$

By the Fundamental Theorem of arithmetic, I need a unique prime factorization

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Assume ½ IS elem

Means $\exists x \in \mathbb{N}$. s.t $\frac{1}{2} = x$

$1 = 2x$

By the Fundamental Theorem of arithmetic, I need a unique prime factorization

factors(1) = [] (none)

Proof by contradiction

Thm: ½ is not an element of the natural numbers

Assume ½ IS elem

Means $\exists x \in \mathbb{N}$. s.t $\frac{1}{2} = x$

$1 = 2x$

By the Fundamental Theorem of arithmetic, I need a unique prime factorization

factors(1) = [] (none)

factors (2x) = [2] along with the factors of x

Proof by contradiction -- Informal

Thm: $\frac{1}{2}$ is not an element of the natural numbers

Assume $\frac{1}{2}$ IS elem

Means $\exists x \in \mathbb{N}$. s.t $\frac{1}{2} = x$

$1 = 2x$

By the Fundamental Theorem of arithmetic, I need a unique prime factorization

factors(1) = [] (none)

factors (2x) = [2] along with the factors of x

One side has zero factors, one has at least 1?? Contradiction

Proof by contradiction -- Formal

Thm: ½ is not an element of the natural numbers

We proceed by contradiction
Assume $\frac{1}{2} \in \mathbb{N}$.
Then, $\exists x \in \mathbb{N}.\ x = \frac{1}{2}$
By algebra, that means $2x = 1$.

By the fundamental theorem of arithmetic, both sides of the equation are equal, so 1 and 2x must have the same unique prime factorization.

But the factors of 2x include 2, and the factors of 1 do not. Therein lies the contradiction.

Therefore, [Because this assumption led to a contradiction,] $\frac{1}{2} \notin \mathbb{N}$

Proof by contradiction

Theorem: Not A

We proceed by contradiction.

Assume A to prove this”

...

A proves FALSE

Therein lies the contradiction.

Therefore

Not A

Often how we prove something is impossible in computing

Rational Numbers -- $\mathbb{Q}$

Represented by $\mathbb{Q}$, which stands for quotient

That's because all rational numbers can be represented by a quotient of two integers! aka an improper (or proper) fraction…

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}$$

Proof by Contradiction -- $\mathbb{Q}$

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}^+$$

Prove by contradiction that $\sqrt{5}$ is not a rational number.

Proof by Contradiction -- $\mathbb{Q}$

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}^+$$

Prove by contradiction that $\sqrt{5}$ is not a rational number.

Assume:

Proof by Contradiction -- $\mathbb{Q}$

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}^{+}$$

Prove by contradiction that $\sqrt{5}$ is not a rational number.

Assume that $\sqrt{5} \in \mathbb{Q}$

By the definition of rational numbers, this means...

Proof by Contradiction -- $\mathbb{Q}$

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}^+$$

Prove by contradiction that √5 is not a rational number.

Assume that $\sqrt{5} \in \mathbb{Q}$

By the definition of rational numbers, this means $\sqrt{5} = \frac{a}{b}$ where both a and b are integers.

Proof by Contradiction -- $\mathbb{Q}$

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}^+$$

Prove by contradiction that √5 is not a rational number.

Assume that $\sqrt{5} \in \mathbb{Q}$

By the definition of rational .numbers, this means $\sqrt{5} = \frac{a}{b}$ where both a and b are integers.

With some arithmetic, $5b^2 = a^2$.

Proof by Contradiction -- $\mathbb{Q}$

By the definition of rational numbers, this means $\sqrt{5} = \frac{a}{b}$ where both a and b are integers.

With some arithmetic, $5b^2 = a^2$. However, $5b^2$ and a^2 are both integers, and adhere to the Fundamental Theorem of Arithmetic.

Since these two numbers are equal, they have to have the same unique prime factorization. However, $5b^2$ must have an **odd multiplicity** of factor 5, while a^2 has an **even multiplicity**, since squaring an integer simply doubles the multiplicity of that integer's original factors.

Because the two numbers are supposed to be equal but do not have the same prime factors, there is a contradiction. This contradiction means that **√5 is not a rational number.**

Proof by Contradiction -- $\mathbb{Q}$

$$x \in \mathbb{Q} \text{ iff } x = \frac{a}{b} \quad \text{where } a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}^+$$

Prove by contradiction that $\sqrt{5}$ is not a rational number.

Assume that $\sqrt{5} \in \mathbb{Q}$

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Theorem: There is no smallest rational number larger than 0.

$$\forall n_1 \in \mathbb{Q}^+ . \exists n_2 \in \mathbb{Q}^+ . n_2 < n_1$$

What's the first step???

We proceed by contradiction

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Negate the theorem!

$$\neg\left(\forall n_1 \in \mathbb{Q}^+ \,.\, \exists n_2 \in \mathbb{Q}^+ \,.\, n_2 < n_1\right)$$

Applying DeMorgan's Laws:

$$\exists n_1 \in \mathbb{Q}^+ \,.\, \nexists n_2 \in \mathbb{Q}^+ \,.\, n_2 < n_1$$

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Negated Theorem:

$$\exists n_1 \in \mathbb{Q}^+ \;.\; \nexists n_2 \in \mathbb{Q}^+ \;.\; n_2 < n_1$$

What does it mean in English?

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Negated Theorem:

$$\exists n_1 \in \mathbb{Q}^+ \,.\, \nexists n_2 \in \mathbb{Q}^+ \,.\, n_2 < n_1$$

“There exists an element in the domain such that there does not exist another element that is less than the first one.

“There exists a smallest positive rational.”

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Negated Theorem:

$$\exists n_1 \in \mathbb{Q}^+ \,.\, \nexists n_2 \in \mathbb{Q}^+ \,.\, n_2 < n_1$$

Because all the numbers are positive rationals, by assigning n2 to be a/2 it will be half as small as n1, we can assert that n2 < n1. But this contradicts our assumption, we stated a smaller positive rational *did not exist* for every positive rational.

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Negated Theorem:

$$\exists n_1 \in \mathbb{Q}^+ \;.\; \nexists n_2 \in \mathbb{Q}^+ \;.\; n_2 < n_1$$

Because all the numbers are positive rationals, by assigning n2 to be a/2 it will be half as small as n1, we can assert that n2 < n1. But this contradicts our assumption, we stated a smaller positive rational *did not exist* for every positive rational.

Our assumption led to a contradiction, since we can always divide a positive rational by another rational to get an even smaller one, as shown above. Because our assumption led to a contradiction, out assumption must be false, and we have proved the theorem.

Proof by Contradiction -- No smallest positive $\mathbb{Q}$

Negated Theorem:

$$\exists n_1 \in \mathbb{Q}^+ \,.\, \nexists n_2 \in \mathbb{Q}^+ \,.\, n_2 < n_1$$

Because all the numbers are positive rationals, by assigning n2 to be a/2 it will be half as small as n1, we can assert that n2 < n1. But this contradicts our assumption, we stated a smaller positive rational *did not exist* for every positive rational.

Our assumption led to a contradiction, since we can always divide a positive rational by another rational to get an even smaller one, as shown above. Because our assumption led to a contradiction, out assumption must be false, and we have proved the theorem.

$$\forall n_1 \in \mathbb{Q}^+ \,.\, \exists n_2 \in \mathbb{Q}^+ \,.\, n_2 < n_1$$

Quiz Question

Provide a counter-example showing that $f(x)=5x$ is **not surjective** given domain and co-domain of $\mathbb{Z}$.

Quiz Question

Provide a counter-example showing that $f(x)=5x$ is **not surjective** given domain and co-domain of $\mathbb{Z}$.

No x in the domain can make $f(x) = -6$

Quiz Question

Provide a counter-example showing that f(x)=5x is **not surjective** given domain and co-domain of $\mathbb{Z}$.

$$\nexists\, x \in \mathbb{Z}.\ (\ f(x) = -6\ )$$

Quiz Question

Prove that f(x)=5x is not a surjective function given domain and co-domain of $\mathbb{Z}$.

$$\nexists\, x \in \mathbb{Z}.\ (\ f(x) = -6\ )$$

Quiz Question

Prove that f(x)=5x is not a surjective function given domain and co-domain of $\mathbb{Z}$.

$$\nexists\, x \in \mathbb{Z}.\ (\ f(x) = -6\ )$$

why is this not enough??

Quiz Question

Prove that $f(x)=5x$ is not a surjective function given domain and co-domain of $\mathbb{Z}$.

Quiz Question

Prove that $f(x)=5x$ is not a surjective function given domain and co-domain of $\mathbb{Z}$.

Suppose $f(x)$ *is* a surjective function.

Quiz Question

Prove that $f(x)=5x$ is not a surjective function given domain and co-domain of $\mathbb{Z}$.

Suppose $f(x)$ *is* a surjective function.

By definition, a function is surjective if its co-domain is the same set as its range.

Quiz Question

Prove that $f(x)=5x$ is not a surjective function given domain and co-domain of $\mathbb{Z}$.

Suppose $f(x)$ *is* a surjective function.

By definition, a function is surjective if its co-domain is the same set as its range.

However, this is not the case for $f(x)$, because there are members of its co-domain that are not part of the function's range; for example, -6 is in the co-domain but not the range.

Quiz Question

Prove that f(x)=5x is not a surjective function given domain and co-domain of $\mathbb{Z}$.

Suppose f(x) *is* a surjective function.

By definition, a function is surjective if its co-domain is the same set as its range.

However, this is not the case for f(x), because there are members of its co-domain that are not part of the function's range; for example, -6 is in the co-domain but not the range.

Therein lies the contradiction. Therefore, f(x) is not a surjective function. ∎

Quiz Question

General structure of proof by contradictions

We’ll start by using some examples from **number theory (the study of integers).**