Intro to the Primes Project

Exposition by William Gasarch

May 21, 2026

What Are The Primes in $\mathbb{N}$?

What Are The Primes in $\mathbb{N}$?

Def $p \in \mathbb{N}$ is **prime** if $p = ab$ implies either $a = 1$ or $b = 1$.

What Are The Primes in $\mathbb{N}$?

Def $p \in \mathbb{N}$ is **prime** if $p = ab$ implies either $a = 1$ or $b = 1$.

Def $p \in \mathbb{N}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

What Are The Primes in $\mathbb{N}$?

Def $p \in \mathbb{N}$ is **prime** if $p = ab$ implies either $a = 1$ or $b = 1$.

Def $p \in \mathbb{N}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Which of these is correct?

What Are The Primes in $\mathbb{N}$?

Def $p \in \mathbb{N}$ is **prime** if $p = ab$ implies either $a = 1$ or $b = 1$.

Def $p \in \mathbb{N}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Which of these is correct?

They are equivalent in $\mathbb{N}$. We will later see domains where these two concept are not equivalent.

What Are The Primes in $\mathbb{N}$?

Def $p \in \mathbb{N}$ is **prime** if $p = ab$ implies either $a = 1$ or $b = 1$.

Def $p \in \mathbb{N}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Which of these is correct?

They are equivalent in $\mathbb{N}$. We will later see domains where these two concept are not equivalent.

Do Prove these are equivalent.

What Are The Primes in $\mathbb{Z}$?

What Are The Primes in $\mathbb{Z}$?

Is -7 primes. Note that $7 = -1 \times -1 \times 7$.

What Are The Primes in $\mathbb{Z}$?

Is -7 primes. Note that $7 = -1 \times -1 \times 7$.

Yes -7 is prime.

What Are The Primes in $\mathbb{Z}$?

Is -7 primes. Note that $7 = -1 \times -1 \times 7$.

Yes -7 is prime. How to define prime. Discuss.

What Are The Primes in $\mathbb{Z}$?

Is -7 primes. Note that $7 = -1 \times -1 \times 7$.

Yes -7 is prime. How to define prime. Discuss.

Definition on next page.

Definition of Primes in $\mathbb{Z}$?

Definition of Primes in $\mathbb{Z}$?

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $a = \pm 1$ or $b = \pm 1$.

Definition of Primes in $\mathbb{Z}$?

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $a = \pm 1$ or $b = \pm 1$.

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $p|a$ or $p|b$.

Definition of Primes in $\mathbb{Z}$?

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $a = \pm 1$ or $b = \pm 1$.

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $p|a$ or $p|b$.

They are equivalent in $\mathbb{Z}$. We will later see domains where these two concept are not equivalent.

Definition of Primes in $\mathbb{Z}$?

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $a = \pm 1$ or $b = \pm 1$.

Def $p \in \mathbb{Z}$ is **prime** if $p = ab$ implies either $p|a$ or $p|b$.

They are equivalent in $\mathbb{Z}$. We will later see domains where these two concept are not equivalent.

Do Prove these are equivalent.

Primes in $\mathbb{Z}[i]$?

Primes in $\mathbb{Z}[i]$?

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Primes in $\mathbb{Z}[i]$?

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Discuss how to define prime in $\mathbb{Z}[i]$.

Primes in $\mathbb{Z}[i]$?

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Discuss how to define prime in $\mathbb{Z}[i]$.

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either

Primes in $\mathbb{Z}[i]$?

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Discuss how to define prime in $\mathbb{Z}[i]$.

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either $a \in \{1, -1, i, -i\}$ or $b \in \{1, -1, i, -i\}$

Primes in $\mathbb{Z}[i]$?

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Discuss how to define prime in $\mathbb{Z}[i]$.

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either
$a \in \{1, -1, i, -i\}$ or $b \in \{1, -1, i, -i\}$

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either $p|a$ or $p|b$.

Primes in $\mathbb{Z}[i]$?

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Discuss how to define prime in $\mathbb{Z}[i]$.

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either
$a \in \{1, -1, i, -i\}$ or $b \in \{1, -1, i, -i\}$

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either $p|a$ or $p|b$.

They are equivalent in $\mathbb{Z}[i]$. We will later see domains where these two concept are not equivalent.

Primes in $\mathbb{Z}[i]$?

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Discuss how to define prime in $\mathbb{Z}[i]$.

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either
$a \in \{1, -1, i, -i\}$ or $b \in \{1, -1, i, -i\}$

Def $p \in \mathbb{Z}[i]$ is **prime** if $p = ab$ implies either $p|a$ or $p|b$.

They are equivalent in $\mathbb{Z}[i]$. We will later see domains where these two concept are not equivalent.

Do Prove these are equivalent.

We Need a Definition to Cover $\mathbb{Z}$ and $\mathbb{Z}[i]$ and ...

We Need a Definition to Cover $\mathbb{Z}$ and $\mathbb{Z}[i]$ and ...

We need a definition of the kind of domains we will be dealing with

Integral Domains

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Note

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Note

Every elt has an add-inv but not every elt has a mult-inv.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Note

Every elt has an add-inv but not every elt has a mult-inv.

$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Note

Every elt has an add-inv but not every elt has a mult-inv.

$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

$\{\frac{a}{b} : b \equiv 1 \pmod 2\}$ is an integral domain. Prove it.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Note

Every elt has an add-inv but not every elt has a mult-inv.

$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

$\{\frac{a}{b} : b \equiv 1 \pmod 2\}$ is an integral domain. Prove it.

$\mathbb{N}$ is not an integral domain and we will not be mentioning it again.

Integral Domains

Def An **Integral Domain** is a set $\mathbb{D}$ with two operations $+, \times$:

$+$ and $\times$ are communicative, associative.

$a \times (b + c) = (a \times b) + (a \times c)$.

There exists $0 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x + 0 = x]$.

There exists $1 \in \mathbb{D}$ with the property that $(\forall x \in \mathbb{D})[x1 = x]$.

For all $x \in \mathbb{D}$ there exists $-x \in \mathbb{D}$ such that $x + (-x) = 0$.

Note

Every elt has an add-inv but not every elt has a mult-inv.

$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

$\{\frac{a}{b} : b \equiv 1 \pmod 2\}$ is an integral domain. Prove it.

$\mathbb{N}$ is not an integral domain and we will not be mentioning it again.

We explore primes in different integral domains.

Units

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.
$\mathbb{U}$ be the set of units.

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.
$\mathbb{U}$ be the set of units.

$\mathbb{Z}$: Units are ± 1.

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.
$\mathbb{U}$ be the set of units.

$\mathbb{Z}$: Units are ± 1.

$\mathbb{Z}[i]$: Units are $1, -1, i, -i$

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.
$\mathbb{U}$ be the set of units.

$\mathbb{Z}$: Units are ± 1.

$\mathbb{Z}[i]$: Units are $1, -1, i, -i$

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: all nonzero elements are units.

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.
$\mathbb{U}$ be the set of units.

$\mathbb{Z}$: Units are ± 1.

$\mathbb{Z}[i]$: Units are $1, -1, i, -i$

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: all nonzero elements are units.

$\{\frac{a}{b} : b \equiv 1 \pmod 2\}$ is an integral domain. Prove it.

Units

Def Let $\mathbb{D}$ be an integral domain. All definitions are relative to $\mathbb{D}$.

A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in D$ with $uv = 1$.
$\mathbb{U}$ be the set of units.

$\mathbb{Z}$: Units are ± 1.

$\mathbb{Z}[i]$: Units are $1, -1, i, -i$

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: all nonzero elements are units.

$\{\frac{a}{b} : b \equiv 1 \pmod 2\}$ is an integral domain. Prove it.

Units are $\{\frac{a}{b} : a, b \equiv 1 \pmod 2\}$. Prove it.

Primes and Irreducibles

Primes and Irreducibles

An **irreducible** is a $p \in \mathbb{D}$ such that if $p = ab$ then $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

Primes and Irreducibles

An **irreducible** is a $p \in \mathbb{D}$ such that if $p = ab$ then $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

A **prime** is a $p \in \mathbb{D}$ such that if p divides ab then p divides a or p divides b.

Primes and Irreducibles

An **irreducible** is a $p \in \mathbb{D}$ such that if $p = ab$ then $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

A **prime** is a $p \in \mathbb{D}$ such that if p divides ab then p divides a or p divides b.

We let $\mathbb{I}$ be the set of irreducibles.

Primes and Irreducibles

An **irreducible** is a $p \in \mathbb{D}$ such that if $p = ab$ then $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

A **prime** is a $p \in \mathbb{D}$ such that if p divides ab then p divides a or p divides b.

We let $\mathbb{I}$ be the set of irreducibles.

Notes

Primes and Irreducibles

An **irreducible** is a $p \in \mathbb{D}$ such that if $p = ab$ then $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

A **prime** is a $p \in \mathbb{D}$ such that if p divides ab then p divides a or p divides b.

We let $\mathbb{I}$ be the set of irreducibles.

Notes

All primes are irreducible but not all irr are primes.

Which Primes Count

Which Primes Count

Imagine that we did not know that $\mathbb{Z}$ had an infinite number of primes.

Which Primes Count

Imagine that we did not know that $\mathbb{Z}$ had an infinite number of primes.

Imagine that we are listing out primes to get an idea.

Which Primes Count

Imagine that we did not know that $\mathbb{Z}$ had an infinite number of primes.

Imagine that we are listing out primes to get an idea.

Do we list out both 7 and -7?

Which Primes Count

Imagine that we did not know that $\mathbb{Z}$ had an infinite number of primes.

Imagine that we are listing out primes to get an idea.

Do we list out both 7 and -7?
No. We think of them as being the same.

Which Primes Count

Imagine that we did not know that $\mathbb{Z}$ had an infinite number of primes.

Imagine that we are listing out primes to get an idea.

Do we list out both 7 and -7?
No. We think of them as being the same.
We impose an equivalence relation on $\mathbb{I}$: p and q are equivalent if there exists $u \in \mathbb{U}$ such that $p = uq$.

Which Primes Count

Imagine that we did not know that $\mathbb{Z}$ had an infinite number of primes.

Imagine that we are listing out primes to get an idea.

Do we list out both 7 and -7?
No. We think of them as being the same.
We impose an equivalence relation on $\mathbb{I}$: p and q are equivalent if there exists $u \in \mathbb{U}$ such that $p = uq$.
We say $\mathbb{I}$ *is infinite up to units* if the number of equivalence classes is infinite.

TO DO

TO DO

Here is your TO DO list

TO DO

Here is your TO DO list

Show that in $\mathbb{Z}[i]$ x is prime iff x is irreducible.

TO DO

Here is your TO DO list

Show that in $\mathbb{Z}[i]$ x is prime iff x is irreducible.

TO DO: If x is composite in $\mathbb{Z}$ then its composite in $\mathbb{Z}[i]$.

TO DO

Here is your TO DO list

Show that in $\mathbb{Z}[i]$ x is prime iff x is irreducible.

TO DO: If x is composite in $\mathbb{Z}$ then its composite in $\mathbb{Z}[i]$.

There are primes in $\mathbb{Z}$ that are not primes in $\mathbb{Z}[i]$:

TO DO

Here is your TO DO list

Show that in $\mathbb{Z}[i]$ x is prime iff x is irreducible.

TO DO: If x is composite in $\mathbb{Z}$ then its composite in $\mathbb{Z}[i]$.

There are primes in $\mathbb{Z}$ that are not primes in $\mathbb{Z}[i]$:
$5 = (2+i)(2-i)$ so 5 is not prime.

TO DO

Here is your TO DO list

Show that in $\mathbb{Z}[i]$ x is prime iff x is irreducible.

TO DO: If x is composite in $\mathbb{Z}$ then its composite in $\mathbb{Z}[i]$.

There are primes in $\mathbb{Z}$ that are not primes in $\mathbb{Z}[i]$:
$5 = (2+i)(2-i)$ so 5 is not prime.
Are $2+i$ and $2-i$ prime?

TO DO

Here is your TO DO list

Show that in $\mathbb{Z}[i]$ x is prime iff x is irreducible.

TO DO: If x is composite in $\mathbb{Z}$ then its composite in $\mathbb{Z}[i]$.

There are primes in $\mathbb{Z}$ that are not primes in $\mathbb{Z}[i]$:
$5 = (2+i)(2-i)$ so 5 is not prime.
Are $2+i$ and $2-i$ prime?
TO DO: Determine exactly which elements of $\mathbb{Z}[i]$ are primes.