Schur's Thm + FLT implies Primes Infinite

May 8, 2025

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.
3. Elsholtz (2021) used INT and Schur's Thm.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.
3. Elsholtz (2021) used INT and Schur's Thm.
4. Goral, Ozcan, Serbas (2022) used HNT and Poly-VDW Thm.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.
3. Elsholtz (2021) used INT and Schur's Thm.
4. Goral, Ozcan, Serbas (2022) used HNT and Poly-VDW Thm.
5. Gasarch (2023) used INT and Schur's Thm.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.
3. Elsholtz (2021) used INT and Schur's Thm.
4. Goral, Ozcan, Serbas (2022) used HNT and Poly-VDW Thm.
5. Gasarch (2023) used INT and Schur's Thm.
6. We refer to the proof by Elsholtz and Gasarch as the **EG-proof**.

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.
3. Elsholtz (2021) used INT and Schur's Thm.
4. Goral, Ozcan, Serbas (2022) used HNT and Poly-VDW Thm.
5. Gasarch (2023) used INT and Schur's Thm.
6. We refer to the proof by Elsholtz and Gasarch as the **EG-proof**.

1. All of these proofs are harder than the usual proof

Credit Where Credit is Due

The following people have used Ramsey Theory to show Primes ∞.

1. Alpoge (2015) used Intermediary NT (INT) and VDW.
2. Granville (2017) used INT and VDW.
3. Elsholtz (2021) used INT and Schur's Thm.
4. Goral, Ozcan, Serbas (2022) used HNT and Poly-VDW Thm.
5. Gasarch (2023) used INT and Schur's Thm.
6. We refer to the proof by Elsholtz and Gasarch as the **EG-proof**.

1. All of these proofs are harder than the usual proof
2. All of these proofs have other points to make after they prove primes ∞.

Plan for Todays Talk

Plan for Todays Talk

1. Present the EG-Proof since its the one I know best.

Plan for Todays Talk

1. Present the EG-Proof since its the one I know best.
2. Look at what it means to ask the question in domains other than $\mathbb{N}$. (In fact, asking it over $\mathbb{N}$ is not quite right).

Plan for Todays Talk

1. Present the EG-Proof since its the one I know best.
2. Look at what it means to ask the question in domains other than $\mathbb{N}$. (In fact, asking it over $\mathbb{N}$ is not quite right).
3. Look at domains where the number of primes is finite and see where the standard proof fails, and where the EG-proof fails.

Background Needed For EG-Proof

May 8, 2025

Notation Needed

Notation Let $k, n \in \mathbb{N} - \{0\}$.

Notation Needed

Notation Let $k, n \in \mathbb{N} - \{0\}$.
Let A be any set (it can even be ∞).

Notation Needed

Notation Let $k, n \in \mathbb{N} - \{0\}$.
Let A be any set (it can even be ∞).

1. $[n] = \{1, 2, \ldots, n\}$.

Notation Needed

Notation Let $k, n \in \mathbb{N} - \{0\}$.
Let A be any set (it can even be ∞).

1. $[n] = \{1, 2, \ldots, n\}$.
2. $\binom{A}{k}$ is the set of all subsets of A of size k.

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \rightarrow [c]$ there exists x, y, z monochromatic such that $x + y = z$.

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \rightarrow [c]$ there exists x, y, z monochromatic such that $x + y = z$.
Pf We determine S later.

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \rightarrow [c]$ there exists x, y, z monochromatic such that $x + y = z$.

Pf We determine S later.

Given COL we define $\mathrm{COL}'\binom{[S]}{2} \rightarrow [c]$ as follows:

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \to [c]$ there exists x, y, z monochromatic such that $x + y = z$.
Pf We determine S later.
Given COL we define $\mathrm{COL}'\binom{[S]}{2} \to [c]$ as follows:

$$\mathrm{COL}'(x, y) = COL(|x - y|).$$

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \rightarrow [c]$ there exists x, y, z monochromatic such that $x + y = z$.
Pf We determine S later.
Given COL we define $\mathrm{COL}'\binom{[S]}{2} \rightarrow [c]$ as follows:

$$\mathrm{COL}'(x, y) = COL(|x - y|).$$

There exists a COL'-homog set H of size 3 (thats all we need!).
Say its $a < b < c$

$$\mathrm{COL}'(c, b) = \mathrm{COL}'(b, a) = \mathrm{COL}'(c, a)$$

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \rightarrow [c]$ there exists x, y, z monochromatic such that $x + y = z$.
Pf We determine S later.
Given COL we define $\mathrm{COL}'\binom{[S]}{2} \rightarrow [c]$ as follows:

$$\mathrm{COL}'(x, y) = COL(|x - y|).$$

There exists a COL'-homog set H of size 3 (thats all we need!).
Say its $a < b < c$

$$\mathrm{COL}'(c, b) = \mathrm{COL}'(b, a) = \mathrm{COL}'(c, a)$$

So

$$\mathrm{COL}(c - b) = COL(b - a) = COL(c - a)$$

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \rightarrow [c]$ there exists x, y, z monochromatic such that $x + y = z$.
Pf We determine S later.
Given COL we define $\mathrm{COL}'\binom{[S]}{2} \rightarrow [c]$ as follows:

$$\mathrm{COL}'(x, y) = COL(|x - y|).$$

There exists a COL'-homog set H of size 3 (thats all we need!).
Say its $a < b < c$

$$\mathrm{COL}'(c, b) = \mathrm{COL}'(b, a) = \mathrm{COL}'(c, a)$$

So

$$\mathrm{COL}(c - b) = COL(b - a) = COL(c - a)$$

Let $x = c - b$, $y = b - a$, $z = c - a$.

Schur's Theorem

Thm $(\forall c)(\exists S = S(c))$ st for all c-colorings $\mathrm{COL}\colon [S] \to [c]$ there exists x, y, z monochromatic such that $x + y = z$.
Pf We determine S later.
Given COL we define $\mathrm{COL}'\binom{[S]}{2} \to [c]$ as follows:

$$\mathrm{COL}'(x, y) = COL(|x - y|).$$

There exists a COL'-homog set H of size 3 (thats all we need!).
Say its $a < b < c$

$$\mathrm{COL}'(c, b) = \mathrm{COL}'(b, a) = \mathrm{COL}'(c, a)$$

So

$$\mathrm{COL}(c - b) = COL(b - a) = COL(c - a)$$

Let $x = c - b$, $y = b - a$, $z = c - a$.
So let $S(c) = R(3; c)$ (homog set 3, colors c).

Fermat's Last Theorem

In 1637 Fermat wrote in the margins of **Arithmetica**, a book on Number Theory by Diophantus, the following (translated from Latin)

Fermat's Last Theorem

In 1637 Fermat wrote in the margins of **Arithmetica**, a book on Number Theory by Diophantus, the following (translated from Latin)

To divide a cube into two cubes, a fourth power, or in general any power whatever above the second into two powers of the same denomination, is impossible, and I have assuredly found a proof of this, but the margin is too narrow to contain it.

Fermat's Last Theorem

In 1637 Fermat wrote in the margins of **Arithmetica**, a book on Number Theory by Diophantus, the following (translated from Latin)

To divide a cube into two cubes, a fourth power, or in general any power whatever above the second into two powers of the same denomination, is impossible, and I have assuredly found a proof of this, but the margin is too narrow to contain it.
In modern terminology:

$$(\forall n \geq 3)(\forall x, y, z \in \mathbb{N} - \{0\})[x^n + y^n \neq z^n].$$

This has come to be known as **Fermat's Last Theorem**.

Did Fermat Have a Proof? Arguments Against

Did Fermat Have a Proof? Arguments Against

1) He proved the $n = 4$ case later in his life. He would not have done this if he had earlier proved the full theorem.

Did Fermat Have a Proof? Arguments Against

1) He proved the $n = 4$ case later in his life. He would not have done this if he had earlier proved the full theorem.

2) Andrew Wiles proved FLT in the early 1990s with techniques far beyond what Fermat could have known.

Did Fermat Have a Proof? Arguments For

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

2) The 11th Dr. Who gave **The real proof** to a group of geniuses to gain their trust.

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

2) The 11th Dr. Who gave **The real proof** to a group of geniuses to gain their trust.

1. He later said that it was Fermat's original proof (possible but unlikely),

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

2) The 11th Dr. Who gave **The real proof** to a group of geniuses to gain their trust.

1. He later said that it was Fermat's original proof (possible but unlikely),
2. but that Fermat didn't write it down since he died in a duel (not true).

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

2) The 11th Dr. Who gave **The real proof** to a group of geniuses to gain their trust.

1. He later said that it was Fermat's original proof (possible but unlikely),
2. but that Fermat didn't write it down since he died in a duel (not true).
   The writers of the show either

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

2) The 11th Dr. Who gave **The real proof** to a group of geniuses to gain their trust.

1. He later said that it was Fermat's original proof (possible but unlikely),
2. but that Fermat didn't write it down since he died in a duel (not true).
   The writers of the show either
   2.1 confused Galois with Fermat, or

Did Fermat Have a Proof? Arguments For

1) The 7th Dr. Who had a 5-line proof that uses Boolean Algebra.

2) The 11th Dr. Who gave **The real proof** to a group of geniuses to gain their trust.

1. He later said that it was Fermat's original proof (possible but unlikely),
2. but that Fermat didn't write it down since he died in a duel (not true).
   The writers of the show either
   2.1 confused Galois with Fermat, or
   2.2 meant to say that Fermat died in a duel in a dual timeline.

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN.

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN. **Whoops**

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN. **Whoops**

In **Star Trek: DSN**, the episode **Facets** which aired on June 12, 1995, Dax says that one of her previous hosts, Tobin, had done *the most creative work on Fermat's Last Theorem since Wiles*.

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN. **Whoops**

In **Star Trek: DSN**, the episode **Facets** which aired on June 12, 1995, Dax says that one of her previous hosts, Tobin, had done *the most creative work on Fermat's Last Theorem since Wiles*.

My guess is that Tobin wrote this limerick:

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN. **Whoops**

In **Star Trek: DSN**, the episode **Facets** which aired on June 12, 1995, Dax says that one of her previous hosts, Tobin, had done *the most creative work on Fermat's Last Theorem since Wiles*.

My guess is that Tobin wrote this limerick:

A challenge for many long ages
Had baffled the savants and sages

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN. **Whoops**

In **Star Trek: DSN**, the episode **Facets** which aired on June 12, 1995, Dax says that one of her previous hosts, Tobin, had done *the most creative work on Fermat's Last Theorem since Wiles*.

My guess is that Tobin wrote this limerick:

A challenge for many long ages
Had baffled the savants and sages

Yet at last came the light
Seems that Fermat was right

More Fiction about Fermat's Last Theorem

In **Star Trek: TNG**, the episode **The Royale** which aired on March 27, 1989, Captain Picard, in the 24th Century is working on Fermat's Last Theorem, which is still OPEN. **Whoops**

In **Star Trek: DSN**, the episode **Facets** which aired on June 12, 1995, Dax says that one of her previous hosts, Tobin, had done *the most creative work on Fermat's Last Theorem since Wiles*.

My guess is that Tobin wrote this limerick:

A challenge for many long ages
Had baffled the savants and sages

Yet at last came the light
Seems that Fermat was right

To the margin add 200 pages.

Proof that Primes are Infinite

May 8, 2025

Proof that Primes are Infinite

Thm The number of primes is infinite.

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL} \colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4), \ldots, a_L \pmod 4))$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.
$x = p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L}$
$y = p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L}$
$z = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.
$x = p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L}$
$y = p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L}$
$z = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$
$x + y = z$

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4), \ldots, a_L \pmod 4))$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L}$
$y = p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L}$
$z = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$

$x + y = z$
$p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L} + p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L} = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L}$
$y = p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L}$
$z = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$

$x + y = z$
$p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L} + p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L} = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$
$p_1^{4x_1} \cdots p_L^{4x_L} + p_1^{4y_1} \cdots p_L^{4y_L} = p_1^{4z_1} \cdots p_L^{4z_n}$

Proof that Primes are Infinite

Thm The number of primes is infinite.
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4), \ldots, a_L \pmod 4))$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L}$
$y = p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L}$
$z = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$

$x + y = z$
$p_1^{4x_1+e_1} \cdots p_L^{4x_L+e_L} + p_1^{4y_1+e_1} \cdots p_L^{4y_L+e_L} = p_1^{4z_1+e_1} \cdots p_L^{4z_n+e_L}$
$p_1^{4x_1} \cdots p_L^{4x_L} + p_1^{4y_1} \cdots p_L^{4y_L} = p_1^{4z_1} \cdots p_L^{4z_n}$
$(p_1^{x_1} \cdots p_L^{x_L})^4 + (p_1^{y_1} \cdots p_L^{y_L})^4 = (p_1^{z_1} \cdots p_L^{z_L})^4$
This violates FLT for $n = 4$.

How to Ask the Question of Primes Infinite

May 8, 2025

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.
2. There is an element $0 \in D$ such that $(\forall x \in D)[x + 0 = x]$.

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.
2. There is an element $0 \in D$ such that $(\forall x \in D)[x + 0 = x]$.
3. There is an element $1 \in D$ such that $(\forall x \in D)[x \times 1 = x]$.

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.
2. There is an element $0 \in D$ such that $(\forall x \in D)[x + 0 = x]$.
3. There is an element $1 \in D$ such that $(\forall x \in D)[x \times 1 = x]$.
4. $+$ and $\times$ are communicative and associative.

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.
2. There is an element $0 \in D$ such that $(\forall x \in D)[x + 0 = x]$.
3. There is an element $1 \in D$ such that $(\forall x \in D)[x \times 1 = x]$.
4. $+$ and $\times$ are communicative and associative.
5. (Key) $(\forall x)(\exists y)[x + y = 0]$.

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.
2. There is an element $0 \in D$ such that $(\forall x \in D)[x + 0 = x]$.
3. There is an element $1 \in D$ such that $(\forall x \in D)[x \times 1 = x]$.
4. $+$ and $\times$ are communicative and associative.
5. (Key) $(\forall x)(\exists y)[x + y = 0]$.
6. (Key) If $ab = 0$ then either $a = 0$ or $b = 0$.

Integral Domains

Def An **Integral Domain** is a set D together with operations $+$, $\times$ such that the following hold

1. D is closed under $+$ and $\times$.
2. There is an element $0 \in D$ such that $(\forall x \in D)[x + 0 = x]$.
3. There is an element $1 \in D$ such that $(\forall x \in D)[x \times 1 = x]$.
4. $+$ and $\times$ are communicative and associative.
5. (Key) $(\forall x)(\exists y)[x + y = 0]$.
6. (Key) If $ab = 0$ then either $a = 0$ or $b = 0$.

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers

$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.

Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$. CANNOT DIVIDE.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$. CANNOT DIVIDE.
Proof that $\mathbb{AI}$ is closed under $+$ and $\times$ is hard.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$. CANNOT DIVIDE.
Proof that $\mathbb{AI}$ is closed under $+$ and $\times$ is hard.

5) $\{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$. CANNOT DIVIDE.
Proof that $\mathbb{AI}$ is closed under $+$ and $\times$ is hard.

5) $\{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$. CANNOT DIVIDE. $\neg\exists \frac{1}{2}$.

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$. CANNOT DIVIDE.
Proof that $\mathbb{AI}$ is closed under $+$ and $\times$ is hard.

5) $\{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$. CANNOT DIVIDE. $\neg\exists \frac{1}{2}$.

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

Integral Domains

Upshot $+, \times, 0, 1$ act as you expect, you can subtract, you might not be able to divide.

Integral Domains

1) $\mathbb{Z}$. CANNOT divide: $\neg(\exists \frac{1}{3})$.

2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. CAN divide.

3) Algebraic Numbers
$\mathbb{AN} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]))[f(a) = 0]$. CAN DIVIDE.
Proof that $\mathbb{AN}$ is closed under $+$ and $\times$ is hard.

4) Algebraic integers
$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1$))[p(a) = 0]\}$. CANNOT DIVIDE.
Proof that $\mathbb{AI}$ is closed under $+$ and $\times$ is hard.

5) $\{\frac{a}{b} : \gcd(a, b) = 1 \land b \equiv 1 \pmod 2\}$. CANNOT DIVIDE. $\neg\exists \frac{1}{2}$.

6) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. CANNOT DIVIDE. $\neg\exists \frac{1}{2}$.

Domains that are NOT Integral Domains

Domains that are NOT Integral Domains

1) $\mathbb{Z}_{12} = \{0, \ldots, 11\}$ with mod 12 math.

Domains that are NOT Integral Domains

1) $\mathbb{Z}_{12} = \{0, \ldots, 11\}$ with mod 12 math.

Note that $3 \times 4 = 0$ but $3 \neq 0$ and $4 \neq 0$.

Domains that are NOT Integral Domains

1) $\mathbb{Z}_{12} = \{0, \ldots, 11\}$ with mod 12 math.

Note that $3 \times 4 = 0$ but $3 \neq 0$ and $4 \neq 0$. (Note: $\mathbb{Z}_n$ is an integral domain iff n is prime.)

Domains that are NOT Integral Domains

1) $\mathbb{Z}_{12} = \{0, \ldots, 11\}$ with mod 12 math.
Note that $3 \times 4 = 0$ but $3 \neq 0$ and $4 \neq 0$. (Note: $\mathbb{Z}_n$ is an integral domain iff n is prime.)

2) $\mathbb{N}$. There is no -3.

Domains that are NOT Integral Domains

1) $\mathbb{Z}_{12} = \{0, \ldots, 11\}$ with mod 12 math.
Note that $3 \times 4 = 0$ but $3 \neq 0$ and $4 \neq 0$. (Note: $\mathbb{Z}_n$ is an integral domain iff n is prime.)

2) $\mathbb{N}$. There is no -3.

We will look at which Integral Domains have an infinite number of primes.

Domains that are NOT Integral Domains

1) $\mathbb{Z}_{12} = \{0, \ldots, 11\}$ with mod 12 math.
Note that $3 \times 4 = 0$ but $3 \neq 0$ and $4 \neq 0$. (Note: $\mathbb{Z}_n$ is an integral domain iff n is prime.)

2) $\mathbb{N}$. There is no -3.

We will look at which Integral Domains have an infinite number of primes.

Will need to ask the question carefully.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

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

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

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

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$. We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$.
   We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$.
   We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.
3. A **prime** is a $p \in \mathbb{D} - \mathbb{U}$ such that if p divides ab then either p divides a or p divides b.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$.
   We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.
3. A **prime** is a $p \in \mathbb{D} - \mathbb{U}$ such that if p divides ab then either p divides a or p divides b.

   In any integral domain all primes are irreducible but not all irreducibles are primes. (We will not be getting into that).

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$.
   We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.
3. A **prime** is a $p \in \mathbb{D} - \mathbb{U}$ such that if p divides ab then either p divides a or p divides b.

   In any integral domain all primes are irreducible but not all irreducibles are primes. (We will not be getting into that).
4. A **composite** is an $n \in \mathbb{D} - \mathbb{U}$ such that there exists $a, b \in \mathbb{D} - \mathbb{U}$, $n = ab$.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$.
   We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.
3. A **prime** is a $p \in \mathbb{D} - \mathbb{U}$ such that if p divides ab then either p divides a or p divides b.

   In any integral domain all primes are irreducible but not all irreducibles are primes. (We will not be getting into that).
4. A **composite** is an $n \in \mathbb{D} - \mathbb{U}$ such that there exists $a, b \in \mathbb{D} - \mathbb{U}$, $n = ab$.

Units are **not** irreducibles. This is why 1, -1 are not primes.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$. We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.
3. A **prime** is a $p \in \mathbb{D} - \mathbb{U}$ such that if p divides ab then either p divides a or p divides b.

   In any integral domain all primes are irreducible but not all irreducibles are primes. (We will not be getting into that).
4. A **composite** is an $n \in \mathbb{D} - \mathbb{U}$ such that there exists $a, b \in \mathbb{D} - \mathbb{U}$, $n = ab$.

Units are **not** irreducibles. This is why 1, -1 are not primes.

We will be concerned with irreducibles, not primes.

Types of Elements in an Integral Domain

Def Let $\mathbb{D}$ be an integral domain.

1. A **unit** is a $u \in \mathbb{D}$ such that there exists $v \in \mathbb{D}$ with $uv = 1$. We let $\mathbb{U}$ be the set of units.
2. An **irreducible** is a $p \in \mathbb{D} - \mathbb{U}$ such that if $p = ab$ then either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
   We let $\mathbb{I}$ be the set of irreducibles.
3. A **prime** is a $p \in \mathbb{D} - \mathbb{U}$ such that if p divides ab then either p divides a or p divides b.

   In any integral domain all primes are irreducible but not all irreducibles are primes. (We will not be getting into that).
4. A **composite** is an $n \in \mathbb{D} - \mathbb{U}$ such that there exists $a, b \in \mathbb{D} - \mathbb{U}$, $n = ab$.

Units are **not** irreducibles. This is why 1, -1 are not primes.

We will be concerned with irreducibles, not primes.

Types of Elts in an ID 0, units, irreducibles, composites.

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

3) Domain is $\mathbb{CI} = \mathbb{Z}[\{e^{2\pi ik/n} : 0 \leq k \leq n\}]$. $e^{2\pi ik/n}$'s are all units.

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

3) Domain is $\mathbb{CI} = \mathbb{Z}[\{e^{2\pi ik/n} : 0 \le k \le n\}]$. $e^{2\pi ik/n}$'s are all units. ($\mathbb{CI}$ stands for **Cyclotomic Integers**.)

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

3) Domain is $\mathbb{CI} = \mathbb{Z}[\{e^{2\pi ik/n} : 0 \le k \le n\}]$. $e^{2\pi ik/n}$'s are all units.
($\mathbb{CI}$ stands for **Cyclotomic Integers**.)
Is the following argument valid or mid:

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

3) Domain is $\mathbb{CI} = \mathbb{Z}[\{e^{2\pi ik/n} : 0 \le k \le n\}]$. $e^{2\pi ik/n}$'s are all units.
($\mathbb{CI}$ stands for **Cyclotomic Integers**.)
Is the following argument valid or mid:
$\mathbb{CI}$ has an infinite number of irreducibles:

$$\{7 \times \zeta_i^n : n \in \mathbb{N}, 0 \le i \le n\}.$$

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

3) Domain is $\mathbb{CI} = \mathbb{Z}[\{e^{2\pi ik/n} : 0 \le k \le n\}]$. $e^{2\pi ik/n}$'s are all units.
($\mathbb{CI}$ stands for **Cyclotomic Integers**.)
Is the following argument valid or mid:
$\mathbb{CI}$ has an infinite number of irreducibles:

$$\{7 \times \zeta_i^n : n \in \mathbb{N}, 0 \le i \le n\}.$$

It seems like this is cheating. Even 7 and -7 seem to be **the same**.

Which Irreducibles are Different?

1) Domain is $\mathbb{Z}$. Are 7 and -7 DIFFERENT irreducibles? Discuss

2) Domain is $\mathbb{Z}[i]$. Are 7, -7, $7i$, $-7i$ DIFFERENT irreducibles? Discuss

3) Domain is $\mathbb{CI} = \mathbb{Z}[\{e^{2\pi ik/n} : 0 \le k \le n\}]$. $e^{2\pi ik/n}$'s are all units. ($\mathbb{CI}$ stands for **Cyclotomic Integers**.)
Is the following argument valid or mid:
$\mathbb{CI}$ has an infinite number of irreducibles:

$$\{7 \times \zeta_i^n : n \in \mathbb{N}, 0 \le i \le n\}.$$

It seems like this is cheating. Even 7 and -7 seem to be **the same**.

What to do? Discuss

Equivalence Classes of Irreducibles

Convention Let $\mathbb{D}$ be an Int Dom with Units $\mathbb{U}$, Irreds $\mathbb{I}$.

Equivalence Classes of Irreducibles

Convention Let $\mathbb{D}$ be an Int Dom with Units $\mathbb{U}$, Irreds $\mathbb{I}$.
We define the following equivalence relation on $\mathbb{I}$:

$$p \equiv q \text{ iff } (\exists u \in \mathbb{U})[p = uq].$$

Equivalence Classes of Irreducibles

Convention Let $\mathbb{D}$ be an Int Dom with Units $\mathbb{U}$, Irreds $\mathbb{I}$.
We define the following equivalence relation on $\mathbb{I}$:

$$p \equiv q \text{ iff } (\exists u \in \mathbb{U})[p = uq].$$

$\mathbb{I}$ is infinite up to units if the number of equivalence classes is infinite.

Equivalence Classes of Irreducibles

Convention Let $\mathbb{D}$ be an Int Dom with Units $\mathbb{U}$, Irreds $\mathbb{I}$.
We define the following equivalence relation on $\mathbb{I}$:

$$p \equiv q \text{ iff } (\exists u \in \mathbb{U})[p = uq].$$

$\mathbb{I}$ is infinite up to units if the number of equivalence classes is infinite.

New Question Given $\mathbb{D}$ try to show that $\mathbb{D}$ has an infinite number of equiv classes or irreducibles.

Equivalence Classes of Irreducibles

Convention Let $\mathbb{D}$ be an Int Dom with Units $\mathbb{U}$, Irreds $\mathbb{I}$.
We define the following equivalence relation on $\mathbb{I}$:

$$p \equiv q \text{ iff } (\exists u \in \mathbb{U})[p = uq].$$

$\mathbb{I}$ is infinite up to units if the number of equivalence classes is infinite.

New Question Given $\mathbb{D}$ try to show that $\mathbb{D}$ has an infinite number of equiv classes or irreducibles.

On theses slides **infinite** will mean **infinite up to units**.

The Normal Proof that Primes are Infinite and Where it Falls Apart

May 8, 2025

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)
Form $N = p_1 \cdots p_n + 1$.

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)
Form $N = p_1 \cdots p_n + 1$. Two Cases.

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)
Form $N = p_1 \cdots p_n + 1$. Two Cases.

1. N is prime. **Done** since, for all $1 \leq i \leq n$, $p_i < N$ so $p_i \neq N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.
2. N is composite. Then $N = ab$ where $a, b \notin \{-1, 1\}$. If a and b are composite then break them down until you get to prime p, p divides N. So $N = Mp$.

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)
Form $N = p_1 \cdots p_n + 1$. Two Cases.

1. N is prime. **Done** since, for all $1 \leq i \leq n$, $p_i < N$ so $p_i \neq N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.
2. N is composite. Then $N = ab$ where $a, b \notin \{-1, 1\}$. If a and b are composite then break them down until you get to prime p, p divides N. So $N = Mp$.
   $Mp = p_1 \cdots p_n + 1$. Take this mod p.

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)
Form $N = p_1 \cdots p_n + 1$. Two Cases.

1. N is prime. **Done** since, for all $1 \le i \le n$, $p_i < N$ so $p_i \ne N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.
2. N is composite. Then $N = ab$ where $a, b \notin \{-1, 1\}$. If a and b are composite then break them down until you get to prime p, p divides N. So $N = Mp$.
   $Mp = p_1 \cdots p_n + 1$. Take this mod p.
   $0 \equiv p_1 \cdots p_n + 1 \pmod{p}$.

Normal Proof that Primes are Infinite

Thm The set of primes in $\mathbb{Z}$ is infinite.
Assume not. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{Z}$.
(Note- if p and $-p$ both appear, we just take p.)
Form $N = p_1 \cdots p_n + 1$. Two Cases.

1. N is prime. **Done** since, for all $1 \le i \le n$, $p_i < N$ so $p_i \ne N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.
2. N is composite. Then $N = ab$ where $a, b \notin \{-1, 1\}$. If a and b are composite then break them down until you get to prime p, p divides N. So $N = Mp$.
   $Mp = p_1 \cdots p_n + 1$. Take this mod p.
   $0 \equiv p_1 \cdots p_n + 1 \pmod{p}$.
   $p \notin \{p_1, \ldots, p_n\}$ since if it was then $0 \equiv 1 \pmod{p}$.

$\mathbb{Q}$ has a Finite Number of Primes

$\mathbb{Q}$ has 0, units, NO primes, NO composites.

$\mathbb{Q}$ has a Finite Number of Primes

$\mathbb{Q}$ has 0, units, NO primes, NO composites.

Where does proof primes ∞ go wrong? Discuss

$\mathbb{Q}$ has a Finite Number of Primes

$\mathbb{Q}$ has 0, units, NO primes, NO composites.

Where does proof primes ∞ go wrong? Discuss

See next slide.

$\mathbb{Q}$ has a Finite Number of Primes

If $p_1, \ldots, p_n$ are **any** set of rationals then $N = p_1 p_2 \cdots p_n + 1$ is a **a unit**.

$\mathbb{Q}$ has a Finite Number of Primes

If $p_1, \ldots, p_n$ are **any** set of rationals then
$N = p_1 p_2 \cdots p_n + 1$ is a **a unit**.

Note that in the proof we considered two cases:
N is prime.
N is composite.

$\mathbb{Q}$ has a Finite Number of Primes

If $p_1, \ldots, p_n$ are **any** set of rationals then
$N = p_1 p_2 \cdots p_n + 1$ is a **a unit**.

Note that in the proof we considered two cases:
N is prime.
N is composite.

We never considered N is a unit.

$\mathbb{Q}$ has a Finite Number of Primes

If $p_1, \ldots, p_n$ are **any** set of rationals then
$N = p_1 p_2 \cdots p_n + 1$ is a **a unit**.

Note that in the proof we considered two cases:
N is prime.
N is composite.

We never considered N is a unit.

Upshot The proof that $\mathbb{Z}$ has an infinite number of primes uses that, for all $p_1 \cdots p_n + 1$ is never a unit.

$\mathbb{Q}_2$ has a Finite Number of Primes

$$\mathbb{Q}_2 = \{\tfrac{a}{b} : \gcd(a,b) = 1 \wedge b \equiv 1 \pmod 2\}.$$

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

Are there any more primes?

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

Are there any more primes? No. I leave that for you to prove.

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

Are there any more primes? No. I leave that for you to prove.

So it looks like $\mathbb{Q}_2$ has an infinite number of primes.

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

Are there any more primes? No. I leave that for you to prove.

So it looks like $\mathbb{Q}_2$ has an infinite number of primes.

BUT all of the primes listed are equivalent. So $\mathbb{Q}_2$ has only one prime.

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

Are there any more primes? No. I leave that for you to prove.

So it looks like $\mathbb{Q}_2$ has an infinite number of primes.

BUT all of the primes listed are equivalent. So $\mathbb{Q}_2$ has only one prime.

So where does the proof that the primes are infinite go wrong? Discuss

$\mathbb{Q}_2$ has a Finite Number of Primes

$\mathbb{Q}_2 = \{\frac{a}{b} : \gcd(a, b) = 1 \wedge b \equiv 1 \pmod 2\}$.

$\mathbb{Q}_2$ has 0.

$\mathbb{Q}_2$ has units: all $\frac{a}{b}$ where $a \equiv 1 \pmod 2$.

$\mathbb{Q}_2$ has primes: $2, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \frac{2}{9}, \ldots$.

Are there any more primes? No. I leave that for you to prove.

So it looks like $\mathbb{Q}_2$ has an infinite number of primes.

BUT all of the primes listed are equivalent. So $\mathbb{Q}_2$ has only one prime.

So where does the proof that the primes are infinite go wrong? Discuss

See next slide.

$\mathbb{Q}_2$ has a Finite Number of Primes

We actually have a list of primes: $\{2\}$.
$N = 2 + 1 = 3$ which is a unit.
So similar to why the proof fails for $\mathbb{Q}$.

$\mathbb{AI}$ has a Finite Number of Primes

$$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff } 1))[p(a) = 0]\}.$$

$\mathbb{AI}$ has a Finite Number of Primes

$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff } 1))[p(a) = 0]\}$.

The units are

$\mathbb{U} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff 1 and constant coeff is } 1)$
$[p(a) = 0]\}$.

$\mathbb{AI}$ has a Finite Number of Primes

$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1))$[p(a) = 0]\}$.

The units are
$\mathbb{U} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1 and constant coeff is 1)
$[p(a) = 0]\}$.
We won't prove or need this.

$\mathbb{AI}$ has a Finite Number of Primes

$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff } 1))[p(a) = 0]\}$.

The units are

$\mathbb{U} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff 1 and constant coeff is } 1)$
$[p(a) = 0]\}$.

We won't prove or need this. Units are not the problem this time.

$\mathbb{AI}$ has a Finite Number of Primes

$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff } 1))[p(a) = 0]\}$.

The units are
$\mathbb{U} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x] \text{ lead coeff 1 and constant coeff is 1})$
$[p(a) = 0]\}$.
We won't prove or need this. Units are not the problem this time.

Give me a number in $\mathbb{AI}$ thats a prime. Discuss.

$\mathbb{AI}$ has a Finite Number of Primes

$\mathbb{AI} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1))$[p(a) = 0]\}$.

The units are
$\mathbb{U} = \{a \in \mathbb{C} : (\exists f(x) \in \mathbb{Z}[x]$ lead coeff 1 and constant coeff is 1)
$[p(a) = 0]\}$.
We won't prove or need this. Units are not the problem this time.

Give me a number in $\mathbb{AI}$ thats a prime. Discuss.

There are no primes. See next slide.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.
$f(p) = p^n + a_{n-1}p^{n-1} + \cdots + a_1 p + a_0 = 0$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.
$f(p) = p^n + a_{n-1}p^{n-1} + \cdots + a_1 p + a_0 = 0$.

Let
$g(x) = x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_1 x^2 + a_0$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.
$f(p) = p^n + a_{n-1}p^{n-1} + \cdots + a_1 p + a_0 = 0$.

Let
$g(x) = x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_1 x^2 + a_0$.
$g(p^{1/2}) = p^n + a_{n-1}p^{n-1} + a_1 p + a_0 = 0$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.
$f(p) = p^n + a_{n-1}p^{n-1} + \cdots + a_1p + a_0 = 0$.

Let
$g(x) = x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_1x^2 + a_0$.
$g(p^{1/2}) = p^n + a_{n-1}p^{n-1} + a_1p + a_0 = 0$.
So $\sqrt{p} \in \mathbb{AI}$.

$\mathbb{AI}$ has no Primes

Let $p \in \mathbb{AI}$. We show that p is not prime.

Note that $p = \sqrt{p} \times \sqrt{p}$. We need to show that $\sqrt{p} \in \mathbb{AI}$.

Let f be poly with lead coeff 1 such that $f(p) = 0$.
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.
$f(p) = p^n + a_{n-1}p^{n-1} + \cdots + a_1 p + a_0 = 0$.

Let
$g(x) = x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_1 x^2 + a_0$.
$g(p^{1/2}) = p^n + a_{n-1}p^{n-1} + a_1 p + a_0 = 0$.
So $\sqrt{p} \in \mathbb{AI}$.

So there are no primes.

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.
Assume $\mathbb{AI}$ has only a finite number of primes. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{AI}$.

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.
Assume $\mathbb{AI}$ has only a finite number of primes. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{AI}$.
Form $N = p_1 \cdots p_n + 1$

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.
Assume $\mathbb{AI}$ has only a finite number of primes. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{AI}$.
Form $N = p_1 \cdots p_n + 1$

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.
Assume $\mathbb{AI}$ has only a finite number of primes. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{AI}$.
Form $N = p_1 \cdots p_n + 1$

1. N prime. **done** since, for all $1 \le i \le n$, $p_i < N$ so $p_i \neq N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.
Assume $\mathbb{AI}$ has only a finite number of primes. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{AI}$.
Form $N = p_1 \cdots p_n + 1$

1. N prime. **done** since, for all $1 \le i \le n$, $p_i < N$ so $p_i \ne N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.
2. N is composite. $N = ab$ where $a, b \notin \mathbb{U}$. If a and b are composite then break them down further until you get prime p, p divides N. So $N = Mp$.

Where does the Proof Break For $\mathbb{AI}$?

Lets revisit the proof.
Assume $\mathbb{AI}$ has only a finite number of primes. Let $\{p_1, \ldots, p_n\}$ be all of the primes in $\mathbb{AI}$.
Form $N = p_1 \cdots p_n + 1$

1. N prime. **done** since, for all $1 \le i \le n$, $p_i < N$ so $p_i \ne N$. N is a prime but not in $\{p_1, \ldots, p_n\}$. Contradiction.
2. N is composite. $N = ab$ where $a, b \notin \mathbb{U}$. If a and b are composite then break them down further until you get prime p, p divides N. So $N = Mp$.
   This is where the proof breaks down! In $\mathbb{AI}$ you can keep going down and never get to a prime.

Example of Infinite Descending Factors

Example

2

Example of Infinite Descending Factors

Example

2

$= 2^{1/2} \times 2^{1/2}$

Example of Infinite Descending Factors

Example

$$
\begin{aligned}
&2 \\
&= 2^{1/2} \times 2^{1/2} \\
&= 2^{1/4} \times 2^{1/4} \times 2^{1/4} \times 2^{1/4} \\
&= 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8}
\end{aligned}
$$

Example of Infinite Descending Factors

Example

2

$= 2^{1/2} \times 2^{1/2}$

$= 2^{1/4} \times 2^{1/4} \times 2^{1/4} \times 2^{1/4}$

$= 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8}$

etc.

Example of Infinite Descending Factors

Example

2
$= 2^{1/2} \times 2^{1/2}$
$= 2^{1/4} \times 2^{1/4} \times 2^{1/4} \times 2^{1/4}$
$= 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8}$
etc.

So what property of $\mathbb{Z}$ was used to avoid this problem?

Example of Infinite Descending Factors

Example

$$2$$
$$= 2^{1/2} \times 2^{1/2}$$
$$= 2^{1/4} \times 2^{1/4} \times 2^{1/4} \times 2^{1/4}$$
$$= 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8} \times 2^{1/8}$$

etc.

So what property of $\mathbb{Z}$ was used to avoid this problem?

See next slide.

Atomic Domains

Def An **Atomic Integral Domain** is an integral domain such that every element of $\mathbb{D} - (\mathbb{U} \cup \{0\})$ can be written (not necessarily uniquely) as $up_1^{x_1} \cdots p_m^{x_m}$ where u is a unit and all of the p_i's are irreducible.

Atomic Domains

Def An **Atomic Integral Domain** is an integral domain such that every element of $\mathbb{D} - (\mathbb{U} \cup \{0\})$ can be written (not necessarily uniquely) as $up_1^{x_1} \cdots p_m^{x_m}$ where u is a unit and all of the p_i's are irreducible.

Examples

$\mathbb{Z}$. Key is that $f(x) = |x|$ is such that $f(a) < f(ab)$ and $f(ab) < f(b)$. So when you factor you end up with smaller numbers.

Atomic Domains

Def An **Atomic Integral Domain** is an integral domain such that every element of $\mathbb{D} - (\mathbb{U} \cup \{0\})$ can be written (not necessarily uniquely) as $up_1^{x_1} \cdots p_m^{x_m}$ where u is a unit and all of the p_i's are irreducible.

Examples

$\mathbb{Z}$. Key is that $f(x) = |x|$ is such that $f(a) < f(ab)$ and $f(ab) < f(b)$. So when you factor you end up with smaller numbers.

$\mathbb{Z}[i]$. Key is that $f(x + iy) = x^2 + y^2$ decreases when you factor.

Atomic Domains

Def An **Atomic Integral Domain** is an integral domain such that every element of $\mathbb{D} - (\mathbb{U} \cup \{0\})$ can be written (not necessarily uniquely) as $up_1^{x_1} \cdots p_m^{x_m}$ where u is a unit and all of the p_i's are irreducible.

Examples

$\mathbb{Z}$. Key is that $f(x) = |x|$ is such that $f(a) < f(ab)$ and $f(ab) < f(b)$. So when you factor you end up with smaller numbers.

$\mathbb{Z}[i]$. Key is that $f(x + iy) = x^2 + y^2$ decreases when you factor.

$\mathbb{AI}$ has no such function (called a Norm).

Atomic Domains

Def An **Atomic Integral Domain** is an integral domain such that every element of $\mathbb{D} - (\mathbb{U} \cup \{0\})$ can be written (not necessarily uniquely) as $up_1^{x_1} \cdots p_m^{x_m}$ where u is a unit and all of the p_i's are irreducible.

Examples

$\mathbb{Z}$. Key is that $f(x) = |x|$ is such that $f(a) < f(ab)$ and $f(ab) < f(b)$. So when you factor you end up with smaller numbers.

$\mathbb{Z}[i]$. Key is that $f(x + iy) = x^2 + y^2$ decreases when you factor.

$\mathbb{AI}$ has no such function (called a Norm).

Upshot The proof that $\mathbb{Z}$ has an infinite number of primes used that $\mathbb{Z}$ is atomic.

The EG-Proof that Primes are Infinite and Where it Falls Apart

May 8, 2025

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
We define a coloring on $N \subseteq \mathbb{Q}$ as follows.

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
We define a coloring on $N \subseteq \mathbb{Q}$ as follows.

Let $\mathrm{COL}\colon \mathbb{N} \to \{0, 1, 2, 3\}^L$ be the following coloring:

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
We define a coloring on $N \subseteq \mathbb{Q}$ as follows.

Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
We define a coloring on $N \subseteq \mathbb{Q}$ as follows.

Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

Two Issues

1) Factoring elements of $\mathbb{N}$ into primes in $\mathbb{N}$ every number is of the form $p_1^{a_1} \cdots p_L^{a_L}$. No issue with units since the only units is 1. We are factoring elements of $\mathbb{N}$ into primes in $\mathbb{Q}$ so units may be needed.

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
We define a coloring on $N \subseteq \mathbb{Q}$ as follows.
Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

Two Issues

1) Factoring elements of $\mathbb{N}$ into primes in $\mathbb{N}$ every number is of the form $p_1^{a_1} \cdots p_L^{a_L}$. No issue with units since the only units is 1. We are factoring elements of $\mathbb{N}$ into primes in $\mathbb{Q}$ so units may be needed.

2) In our proof we used mod 4. Lets keep it n for now and try to pick some n that will work.

Where Does EG-Proof Fail for $\mathbb{Q}$?

Thm The number of primes in $\mathbb{Q}$ is infinite (attempt).
Assume, BWOC, that the primes are finite. $p_1, \ldots, p_L$.
We define a coloring on $N \subseteq \mathbb{Q}$ as follows.
Let $\mathrm{COL}\colon \mathbb{N} \to \{0,1,2,3\}^L$ be the following coloring:

$$\mathrm{COL}(p_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod 4, \ldots, a_L \pmod 4)$$

Two Issues

1) Factoring elements of $\mathbb{N}$ into primes in $\mathbb{N}$ every number is of the form $p_1^{a_1} \cdots p_L^{a_L}$. No issue with units since the only units is 1. We are factoring elements of $\mathbb{N}$ into primes in $\mathbb{Q}$ so units may be needed.

2) In our proof we used mod 4. Lets keep it n for now and try to pick some n that will work.

We define the coloring as follows:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod n, \ldots, a_L \pmod n)$$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod{n}, \ldots, a_L \pmod{n})$$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \to \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod{n}, \ldots, a_L \pmod{n})$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \to \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod{n}, \ldots, a_L \pmod{n})$$

By Schur's Thm there exists x, y, z same color with $x + y = z$. Assume the color is $(e_1, \ldots, e_L)$.

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \to \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod{n}, \ldots, a_L \pmod{n})$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = u_x p_1^{nx_1+e_1} \cdots p_L^{nx_L+e_L}$
$y = u_y p_1^{ny_1+e_1} \cdots p_L^{ny_L+e_L}$
$z = u_z p_1^{nz_1+e_1} \cdots p_L^{nz_n+e_L}$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod{n}, \ldots, a_L \pmod{n})$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = u_x p_1^{nx_1+e_1} \cdots p_L^{nx_L+e_L}$
$y = u_y p_1^{ny_1+e_1} \cdots p_L^{ny_L+e_L}$
$z = u_z p_1^{nz_1+e_1} \cdots p_L^{nz_n+e_L}$

$x + y = z$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \to \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod n, \ldots, a_L \pmod n)$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = u_x p_1^{nx_1+e_1} \cdots p_L^{nx_L+e_L}$
$y = u_y p_1^{ny_1+e_1} \cdots p_L^{ny_L+e_L}$
$z = u_z p_1^{nz_1+e_1} \cdots p_L^{nz_n+e_L}$

$x + y = z$
$u_x p_1^{nx_1+e_1} \cdots p_L^{nx_L+e_L} + p_1^{ny_1+e_1} \cdots p_L^{ny_L+e_L} = u_x p_1^{nz_1+e_1} \cdots p_L^{nz_n+e_L}$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0,\ldots,n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1}\cdots p_L^{a_L}) = (a_1 \pmod{n},\ldots,a_L \pmod{n})$$

By Schur's Thm there exists x,y,z same color with $x+y=z$.
Assume the color is $(e_1,\ldots,e_L)$.

$x = u_x p_1^{nx_1+e_1}\cdots p_L^{nx_L+e_L}$
$y = u_y p_1^{ny_1+e_1}\cdots p_L^{ny_L+e_L}$
$z = u_z p_1^{nz_1+e_1}\cdots p_L^{nz_n+e_L}$

$x+y=z$
$u_x p_1^{nx_1+e_1}\cdots p_L^{nx_L+e_L} + p_1^{ny_1+e_1}\cdots p_L^{ny_L+e_L} = u_x p_1^{nz_1+e_1}\cdots p_L^{nz_n+e_L}$
$u_y p_1^{nx_1}\cdots p_L^{nx_L} + p_1^{ny_1}\cdots p_L^{ny_L} = u_y p_1^{nz_1}\cdots p_L^{nz_n}$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \to \{0,\ldots,n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1}\cdots p_L^{a_L}) = (a_1 \pmod n, \ldots, a_L \pmod n)$$

By Schur's Thm there exists x, y, z same color with $x+y=z$.
Assume the color is $(e_1,\ldots,e_L)$.

$x = u_x p_1^{nx_1+e_1}\cdots p_L^{nx_L+e_L}$
$y = u_y p_1^{ny_1+e_1}\cdots p_L^{ny_L+e_L}$
$z = u_z p_1^{nz_1+e_1}\cdots p_L^{nz_n+e_L}$

$x+y=z$
$u_x p_1^{nx_1+e_1}\cdots p_L^{nx_L+e_L} + p_1^{ny_1+e_1}\cdots p_L^{ny_L+e_L} = u_x p_1^{nz_1+e_1}\cdots p_L^{nz_n+e_L}$
$u_y p_1^{nx_1}\cdots p_L^{nx_L} + p_1^{ny_1}\cdots p_L^{ny_L} = u_y p_1^{nz_1}\cdots p_L^{nz_n}$
$u_x(p_1^{x_1}\cdots p_L^{x_L})^n + u_y(p_1^{y_1}\cdots p_L^{y_L})^n = u_z(p_1^{z_1}\cdots p_L^{z_L})^n$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

Let $\mathrm{COL}\colon \mathbb{N} \rightarrow \{0, \ldots, n-1\}^L$ be the following coloring:

$$\mathrm{COL}(up_1^{a_1} \cdots p_L^{a_L}) = (a_1 \pmod{n}, \ldots, a_L \pmod{n})$$

By Schur's Thm there exists x, y, z same color with $x + y = z$.
Assume the color is $(e_1, \ldots, e_L)$.

$x = u_x p_1^{nx_1+e_1} \cdots p_L^{nx_L+e_L}$
$y = u_y p_1^{ny_1+e_1} \cdots p_L^{ny_L+e_L}$
$z = u_z p_1^{nz_1+e_1} \cdots p_L^{nz_n+e_L}$

$x + y = z$
$u_x p_1^{nx_1+e_1} \cdots p_L^{nx_L+e_L} + p_1^{ny_1+e_1} \cdots p_L^{ny_L+e_L} = u_x p_1^{nz_1+e_1} \cdots p_L^{nz_n+e_L}$
$u_y p_1^{nx_1} \cdots p_L^{nx_L} + p_1^{ny_1} \cdots p_L^{ny_L} = u_y p_1^{nz_1} \cdots p_L^{nz_n}$
$u_x (p_1^{x_1} \cdots p_L^{x_L})^n + u_y (p_1^{y_1} \cdots p_L^{y_L})^n = u_z (p_1^{z_1} \cdots p_L^{z_L})^n$
$u_x X^n + u_y Y^n = u_z Z^n.$

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

We need that there is an n such that

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

We need that there is an n such that
for all $u_x, u_y, u_z \in U$ and $a, b, c \in \mathbb{Q}$

$$u_x X^n + u_y Y^n = u_z Z^n$$

has no solution.

Where Does EG-Proof Fail for $\mathbb{Q}$? (cont)

We need that there is an n such that
for all $u_x, u_y, u_z \in U$ and $a, b, c \in \mathbb{Q}$

$$u_x X^n + u_y Y^n = u_z Z^n$$

has no solution.
Not True Fix n. Let $u_x = u_y = \frac{1}{2}$, $u_z = 1$, $X = Y = Z = 1$.

$$u_x X^n + u_y Y^n = u_z Z^n$$

Becomes

$$\frac{1}{2}1^n + \frac{1}{2}1^n = 1 \times 1^n$$

$$\frac{1}{2} + \frac{1}{2} = 1$$

Where Does EG-Proof Fail for $\mathbb{Q}$?: Upshot

The EG-proof that there are an infinite number of primes (in $\mathbb{N}$) did not transfer to $\mathbb{Q}$ because

Where Does EG-Proof Fail for $\mathbb{Q}$?: Upshot

The EG-proof that there are an infinite number of primes (in $\mathbb{N}$) did not transfer to $\mathbb{Q}$ because
Its NOT that **FLT** is false over $\mathbb{Q}$. Indeed—FLT is true over $\mathbb{Q}$ (follows form FLT being true over $\mathbb{Z}$).

Where Does EG-Proof Fail for $\mathbb{Q}$?: Upshot

The EG-proof that there are an infinite number of primes (in $\mathbb{N}$) did not transfer to $\mathbb{Q}$ because
Its NOT that **FLT** is false over $\mathbb{Q}$. Indeed—FLT is true over $\mathbb{Q}$ (follows form FLT being true over $\mathbb{Z}$).

Its because the following **variant** of FLT is false for $\mathbb{Q}$:

Where Does EG-Proof Fail for $\mathbb{Q}$?: Upshot

The EG-proof that there are an infinite number of primes (in $\mathbb{N}$) did not transfer to $\mathbb{Q}$ because
Its NOT that **FLT** is false over $\mathbb{Q}$. Indeed—FLT is true over $\mathbb{Q}$ (follows form FLT being true over $\mathbb{Z}$).

Its because the following **variant** of FLT is false for $\mathbb{Q}$:

There exists $n \in \mathbb{N}$ such that the following has no solution:

$$u_x X^n + u_y Y^n = u_z Z^n$$

where $u_x, u_y, y_z \in \mathbb{U}$ and $X, Y, Z \in \mathbb{Q}$.

Project TO-DO List

May 8, 2025

Project TO-DO List

Project TO-DO List

1. Read the Gasarch paper. Note that its initial proof was a generalization of what was presented here.

Project TO-DO List

1. Read the Gasarch paper. Note that its initial proof was a generalization of what was presented here.
2. Read in Gasarch's paper the **Sanity Check** which has more domains with a finite number of primes.

Project TO-DO List

1. Read the Gasarch paper. Note that its initial proof was a generalization of what was presented here.
2. Read in Gasarch's paper the **Sanity Check** which has more domains with a finite number of primes.
3. Read the other papers on the website of Ramsey-Primes paper. Some of the papers are difficult so try to just figure out the proof for $\mathbb{Z}$ or $\mathbb{N}$, and then see where it fails for $\mathbb{Q}$ and $\mathbb{Q}_2$. (I think they all fail for $\mathbb{AI}$ because $\mathbb{AI}$ is not atomic, though check that.)