Primes and Irreducibles

Exposition by William Gasarch

June 8, 2026

What Are The Primes? What are Irreducibles?

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.
Since p is prime we have $p|a$ or $p|b$. We assume $p|a$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.
Since p is prime we have $p|a$ or $p|b$. We assume $p|a$.
So there exists $q \in \mathbb{D}$, $a = pq$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.
Since p is prime we have $p|a$ or $p|b$. We assume $p|a$.
So there exists $q \in \mathbb{D}$, $a = pq$.
Since $p = ab$ we have $p = pqb$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.
Since p is prime we have $p|a$ or $p|b$. We assume $p|a$.
So there exists $q \in \mathbb{D}$, $a = pq$.
Since $p = ab$ we have $p = pqb$.
Hence $bq = 1$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.
Since p is prime we have $p|a$ or $p|b$. We assume $p|a$.
So there exists $q \in \mathbb{D}$, $a = pq$.
Since $p = ab$ we have $p = pqb$.
Hence $bq = 1$.
Therefore $b \in \mathbb{U}$.

What Are The Primes? What are Irreducibles?

Def Let $\mathbb{D}$ be a domain. Let $\mathbb{U}$ be the units of $\mathbb{D}$.
1) $p \in \mathbb{D}$ is **irreducible** if $p = ab$ implies either $a \in \mathbb{U}$ or $b \in \mathbb{U}$.
2) $p \in \mathbb{D}$ is **prime** if $p|ab$ implies either $p|a$ or $p|b$.

Thm If p is prime then p is irreducible.
Let p be prime. We show p is irred. Assume $p = ab$. Then $p|ab$.
Since p is prime we have $p|a$ or $p|b$. We assume $p|a$.
So there exists $q \in \mathbb{D}$, $a = pq$.
Since $p = ab$ we have $p = pqb$.
Hence $bq = 1$.
Therefore $b \in \mathbb{U}$.

Question Is the converse true? Are all irreducibles primes?

What Does Divide Mean?

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.

Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.

Example With Units Is $7|-7$ true? Yes.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7| - 7$ true? Yes.
$-7 = 7 \times -1$

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.

Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.

Example With Units Is $7| - 7$ true? Yes.

$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7|-7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7|-7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$. Then $ab = pc$

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7| - 7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$. Then $ab = pc$
Lets say that $a \in \mathbb{U}$.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7|-7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$. Then $ab = pc$
Lets say that $a \in \mathbb{U}$.
Multiply both sides of $ab = pc$ by a^{-1} to get

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7|-7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$. Then $ab = pc$
Lets say that $a \in \mathbb{U}$.
Multiply both sides of $ab = pc$ by a^{-1} to get
$b = pca^{-1}$.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7|-7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$. Then $ab = pc$
Lets say that $a \in \mathbb{U}$.
Multiply both sides of $ab = pc$ by a^{-1} to get
$b = pca^{-1}$. So p divides b.

What Does Divide Mean?

All elements on this slide are in domain $\mathbb{D}$.
Def $p|a$ means that there is a $c \in \mathbb{D}$ such that $a = pc$.
Example With Units Is $7|-7$ true? Yes.
$-7 = 7 \times -1$

The definition of prime is that if $p|ab$ then $p|a$ or $p|b$.
Assume $p|ab$. Then $ab = pc$
Lets say that $a \in \mathbb{U}$.
Multiply both sides of $ab = pc$ by a^{-1} to get
$b = pca^{-1}$. So p divides b.

Upshot If $p|ab$ and one of a or b is a unit then $p|a$ or $p|b$.

In $\mathbb{Z}$ all irreducibles are primes

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$. Mult by b

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$. Mult by b
$abx + pyb = b$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$. Mult by b
$abx + pyb = b$. Since $p|ab$, $ab = pc$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$. Mult by b
$abx + pyb = b$. Since $p|ab$, $ab = pc$.
$pcx + pyb = b$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$. Mult by b
$abx + pyb = b$. Since $p|ab$, $ab = pc$.
$pcx + pyb = b$.
$p(cx + yby) = b$.

In $\mathbb{Z}$ all irreducibles are primes

Thm In $\mathbb{Z}$ all irreducibles are primes.

Let p be an irreducible in $\mathbb{Z}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 a is a unit. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a = \pm 1$ or $c = \pm 1$.
If $a = \pm 1$ then a is a unit so we are done.
If $c = \pm 1$. Then $p = \pm a$ so $p|a$. Done.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
So there exists $x, y \in \mathbb{Z}$ such that
$ax + py = 1$. Mult by b
$abx + pyb = b$. Since $p|ab$, $ab = pc$.
$pcx + pyb = b$.
$p(cx + yby) = b$. So $p|b$.

In $\mathbb{D}$ all irreducibles are primes

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.
If $c \in \mathbb{U}$. Then $p = ca$ so $a = c^{-1}p$ so $p|a$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.
If $c \in \mathbb{U}$. Then $p = ca$ so $a = c^{-1}p$ so $p|a$.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.
If $c \in \mathbb{U}$. Then $p = ca$ so $a = c^{-1}p$ so $p|a$.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
$ax + py = 1$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.
If $c \in \mathbb{U}$. Then $p = ca$ so $a = c^{-1}p$ so $p|a$.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
$ax + py = 1$. Or maybe $ax + py \in \mathbb{U}$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.
If $c \in \mathbb{U}$. Then $p = ca$ so $a = c^{-1}p$ so $p|a$.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
$ax + py = 1$. Or maybe $ax + py \in \mathbb{U}$.
The theorem $\gcd(a, p) = 1$ then $(\exists x, y)[ax + py = 1]$ is true in $\mathbb{Z}$.

In $\mathbb{D}$ all irreducibles are primes

Thm In $\mathbb{D}$ all irreducibles are primes (not true).

Let p be an irreducible in $\mathbb{D}$. We show p is prime.
Assume $p|ab$.
Case 1 $p|a$. Then we are done.
Case 2 $a \in \mathbb{U}$. Then we are done.
Case 3 a divides p. Then $p = ac$.
Since p is irreducible either $a \in \mathbb{U}$ or $c \in \mathbb{U}$.
If $a \in \mathbb{U}$ then we are done.
If $c \in \mathbb{U}$. Then $p = ca$ so $a = c^{-1}p$ so $p|a$.
Case 4 a and p are coprime. Then $\gcd(a, p) = 1$.
$ax + py = 1$. Or maybe $ax + py \in \mathbb{U}$.
The theorem $\gcd(a, p) = 1$ then $(\exists x, y)[ax + py = 1]$ is true in $\mathbb{Z}$.
In what other domains is this true?

A Domain Where Irreducibles and Not Necc Primes

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5}$

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5}$

$ac - 5bd = 2$

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5}$

$ac - 5bd = 2$

$bc + ad = 0.$

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5}$

$ac - 5bd = 2$

$bc + ad = 0$. So $bc = -ad$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5}$

$ac - 5bd = 2$

$bc + ad = 0$. So $bc = -ad$.

Messy! We need better tools for these problems.

Norms

Norms

Let $d \geq 2$ and squarefree.

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Thm $N(xy) = N(x)N(y)$.

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Thm $N(xy) = N(x)N(y)$.

Let $x = x_1 + x_2\sqrt{-d}$ and $y = y_1 + y_2\sqrt{-d}$.

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Thm $N(xy) = N(x)N(y)$.

Let $x = x_1 + x_2\sqrt{-d}$ and $y = y_1 + y_2\sqrt{-d}$.

Could plug all of that in to show $N(xy) = N(x)N(y)$.

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Thm $N(xy) = N(x)N(y)$.

Let $x = x_1 + x_2\sqrt{-d}$ and $y = y_1 + y_2\sqrt{-d}$.

Could plug all of that in to show $N(xy) = N(x)N(y)$.

Messy!

Norms

Let $d \geq 2$ and squarefree. Let $\mathbb{D} = \{a + b\sqrt{-d} \colon a, b \in \mathbb{Z}\}$.

Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Thm $N(xy) = N(x)N(y)$.

Let $x = x_1 + x_2\sqrt{-d}$ and $y = y_1 + y_2\sqrt{-d}$.

Could plug all of that in to show $N(xy) = N(x)N(y)$.

Messy!

See next page for neater way to do it.

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(x) = x\overline{x}$.

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(x) = x\overline{x}$.
Easy to check these two definitions are equivalent.

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.
Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.
Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(x) = x\overline{x}$.
Easy to check these two definitions are equivalent.

Thm $\overline{xy} = \overline{x}\ \overline{y}$.
Easy to check.

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.
Def $N\colon \mathbb{D} \to \mathbb{N}$ is defined by $N(x) = x\overline{x}$.
Easy to check these two definitions are equivalent.

Thm $\overline{xy} = \overline{x}\ \overline{y}$.
Easy to check.

Thm $N(xy) = N(x)N(y)$

Norms: $N(xy) = N(x)N(y)$

Def If $x = x_1 + x_2\sqrt{-d}$ then $\overline{x} = x_1 - x_2\sqrt{-d}$.
Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(a + b\sqrt{-d}) = a^2 + db^2$.
Def $N \colon \mathbb{D} \to \mathbb{N}$ is defined by $N(x) = x\overline{x}$.
Easy to check these two definitions are equivalent.

Thm $\overline{xy} = \overline{x}\ \overline{y}$.
Easy to check.

Thm $N(xy) = N(x)N(y)$

$N(xy) = xy\overline{xy} = xy\overline{x}\ \overline{y} = x\overline{x}y\overline{y} = N(x)N(y)$.

Norms and Units

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$. So $N(x) = 1$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$. So $N(x) = 1$.
$N(x) = 1$: Let $x = a + b\sqrt{-d}$. So $a^2 + db^2 = 1$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$. So $N(x) = 1$.
$N(x) = 1$: Let $x = a + b\sqrt{-d}$. So $a^2 + db^2 = 1$.
Cases show $a = 1$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$. So $N(x) = 1$.
$N(x) = 1$: Let $x = a + b\sqrt{-d}$. So $a^2 + db^2 = 1$.
Cases show $a = 1$.
Thm If x is reducible then $N(x)$ is reducible.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$. So $N(x) = 1$.
$N(x) = 1$: Let $x = a + b\sqrt{-d}$. So $a^2 + db^2 = 1$.
Cases show $a = 1$.
Thm If x is reducible then $N(x)$ is reducible.
If x is reducible then $x = yz$ for $y, z \notin \mathbb{U}$.

Norms and Units

Thm $x \in \mathbb{U}$ iff $N(x) = 1$.
$x \in \mathbb{U}$: $(\exists x^{-1})$.
$1 = N(1) = N(xx^{-1}) = N(x)(N(x^{-1})$. So $N(x) = 1$.
$N(x) = 1$: Let $x = a + b\sqrt{-d}$. So $a^2 + db^2 = 1$.
Cases show $a = 1$.
Thm If x is reducible then $N(x)$ is reducible.
If x is reducible then $x = yz$ for $y, z \notin \mathbb{U}$.
$N(x) = N(y)N(z)$. Since $y, z \notin \mathbb{U}$, $N(y) \neq 1$ and $N(z) \neq 1$ so $N(x)$ is reducible.

A Domain Where Irreducibles and Not Necc Primes

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

Assume, BWOC, that 2 is reducible. So $2 = xy$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.
Assume, BWOC, that 2 is reducible. So $2 = xy$.
$N(2) = N(xy)$

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.
Assume, BWOC, that 2 is reducible. So $2 = xy$.
$N(2) = N(xy)$
$4 = N(x)N(y)$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.
Assume, BWOC, that 2 is reducible. So $2 = xy$.
$N(2) = N(xy)$
$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

Assume, BWOC, that 2 is reducible. So $2 = xy$.

$N(2) = N(xy)$

$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.

If $N(x) = 1$ then $x \in \mathbb{U}$. Done.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

Assume, BWOC, that 2 is reducible. So $2 = xy$.

$N(2) = N(xy)$

$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.

If $N(x) = 1$ then $x \in \mathbb{U}$. Done.

If $N(x) = 4$ then $N(y) = 1$ so $y \in \mathbb{U}$. Done.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.
Assume, BWOC, that 2 is reducible. So $2 = xy$.
$N(2) = N(xy)$
$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.
If $N(x) = 1$ then $x \in \mathbb{U}$. Done.
If $N(x) = 4$ then $N(y) = 1$ so $y \in \mathbb{U}$. Done.
If $N(x) = 2$ then $x = a + b\sqrt{-5}$ and $2 = a^2 + 5b^2$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

Assume, BWOC, that 2 is reducible. So $2 = xy$.

$N(2) = N(xy)$

$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.

If $N(x) = 1$ then $x \in \mathbb{U}$. Done.

If $N(x) = 4$ then $N(y) = 1$ so $y \in \mathbb{U}$. Done.

If $N(x) = 2$ then $x = a + b\sqrt{-5}$ and $2 = a^2 + 5b^2$.

Easy to show $2 = a^2 + 5b^2$ has no solutions in $\mathbb{Z}$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.
Assume, BWOC, that 2 is reducible. So $2 = xy$.
$N(2) = N(xy)$
$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.
If $N(x) = 1$ then $x \in \mathbb{U}$. Done.
If $N(x) = 4$ then $N(y) = 1$ so $y \in \mathbb{U}$. Done.
If $N(x) = 2$ then $x = a + b\sqrt{-5}$ and $2 = a^2 + 5b^2$.
Easy to show $2 = a^2 + 5b^2$ has no solutions in $\mathbb{Z}$.
Upshot 2 is irreducible.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is irreducible.

Assume, BWOC, that 2 is reducible. So $2 = xy$.

$N(2) = N(xy)$

$4 = N(x)N(y)$. So $N(x) \in \{1, 2, 4\}$.

If $N(x) = 1$ then $x \in \mathbb{U}$. Done.

If $N(x) = 4$ then $N(y) = 1$ so $y \in \mathbb{U}$. Done.

If $N(x) = 2$ then $x = a + b\sqrt{-5}$ and $2 = a^2 + 5b^2$.

Easy to show $2 = a^2 + 5b^2$ has no solutions in $\mathbb{Z}$.

Upshot 2 is irreducible.

Next Slide Shows 2 is not prime.

A Domain Where Irreducibles and Not Necc Primes

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.

We show that 2 does not divide $1 + \sqrt{-5}$.

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

2 divides $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$.

We show that 2 does not divide $1+\sqrt{-5}$.

If 2 divides $1+\sqrt{-5}$ then there exists $z \in \mathbb{D}$ such that

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.

We show that 2 does not divide $1 + \sqrt{-5}$.

If 2 divides $1 + \sqrt{-5}$ then there exists $z \in \mathbb{D}$ such that
$1 + \sqrt{-5} = 2z$

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.

We show that 2 does not divide $1 + \sqrt{-5}$.

If 2 divides $1 + \sqrt{-5}$ then there exists $z \in \mathbb{D}$ such that
$1 + \sqrt{-5} = 2z$
$z = \frac{1+\sqrt{-5}}{2}$

A Domain Where Irreducibles and Not Necc Primes

Let $\mathbb{D} = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

2 is not prime.

2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.

We show that 2 does not divide $1 + \sqrt{-5}$.

If 2 divides $1 + \sqrt{-5}$ then there exists $z \in \mathbb{D}$ such that
$1 + \sqrt{-5} = 2z$
$z = \frac{1+\sqrt{-5}}{2}$
AH-$z \notin \mathbb{D}$. Contradiction.

What About the Gaussian Integers?

What About the Gaussian Integers?

Let $\mathbb{D} = \{a + bi \colon a, b \in \mathbb{Z}\}$.

What About the Gaussian Integers?

Let $\mathbb{D} = \{a + bi : a, b \in \mathbb{Z}\}$.

Vote

What About the Gaussian Integers?

Let $\mathbb{D} = \{a + bi : a, b \in \mathbb{Z}\}$.

Vote

In $\mathbb{D}$ all irreducibles are primes.

What About the Gaussian Integers?

Let $\mathbb{D} = \{a + bi : a, b \in \mathbb{Z}\}$.

Vote

In $\mathbb{D}$ all irreducibles are primes.

In $\mathbb{D}$ there are irreducibles that are not prime.

What About the Gaussian Integers?

Let $\mathbb{D} = \{a + bi : a, b \in \mathbb{Z}\}$.

Vote

In $\mathbb{D}$ all irreducibles are primes.

In $\mathbb{D}$ there are irreducibles that are not prime.

The question is UNKNOWN TO SCIENCE.

What About the Gaussian Integers?

Let $\mathbb{D} = \{a + bi : a, b \in \mathbb{Z}\}$.

Vote

In $\mathbb{D}$ all irreducibles are primes.

In $\mathbb{D}$ there are irreducibles that are not prime.

The question is UNKNOWN TO SCIENCE.

Answer on the next slide.

Here is what we Know

Here is what we Know

In $\{a + b\sqrt{-1} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.

Here is what we Know

In $\{a + b\sqrt{-1} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-2} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.

Here is what we Know

In $\{a + b\sqrt{-1} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-2} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-3} \colon a, b \in \mathbb{Z}\}$ There are Irred that are not Primes.

Here is what we Know

In $\{a + b\sqrt{-1} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-2} \colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-3} \colon a, b \in \mathbb{Z}\}$ There are Irred that are not Primes.
In $\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$ There are Irred that are not Prime.

Here is what we Know

In $\{a+b\sqrt{-1}\colon a,b\in\mathbb{Z}\}$ All Irred are Primes.
In $\{a+b\sqrt{-2}\colon a,b\in\mathbb{Z}\}$ All Irred are Primes.
In $\{a+b\sqrt{-3}\colon a,b\in\mathbb{Z}\}$ There are Irred that are not Primes.
In $\{a+b\sqrt{-5}\colon a,b\in\mathbb{Z}\}$ There are Irred that are not Prime.

$d\geq 6$, d squarefree. $\{a+b\sqrt{-d}\colon a,b\in\mathbb{Z}\}$ There are Irred that are not Prime.

Here is what we Know

In $\{a + b\sqrt{-1}\colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-2}\colon a, b \in \mathbb{Z}\}$ All Irred are Primes.
In $\{a + b\sqrt{-3}\colon a, b \in \mathbb{Z}\}$ There are Irred that are not Primes.
In $\{a + b\sqrt{-5}\colon a, b \in \mathbb{Z}\}$ There are Irred that are not Prime.

$d \geq 6$, d squarefree. $\{a + b\sqrt{-d}\colon a, b \in \mathbb{Z}\}$ There are Irred that are not Prime.
We will prove this for $d = 1$ next time (or I'll have you look it up).