Numbers and Primes and Units, Oh My!

PRIMES over $\mathbb{N}$

I want to say that $x \in \mathbb{N}$ is PRIME.

PRIMES over $\mathbb{N}$

I want to say that $x \in \mathbb{N}$ is PRIME.
Quantifiers range over $\mathbb{N}$.

PRIMES over $\mathbb{N}$

I want to say that $x \in \mathbb{N}$ is PRIME.
Quantifiers range over $\mathbb{N}$.

$$\mathrm{PRIME}(x) \equiv (x \neq \{0, 1\}) \wedge (\forall y, z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

PRIMES over $\mathbb{Z}$

I want to say that $x \in \mathbb{Z}$ is PRIME.

PRIMES over $\mathbb{Z}$

I want to say that $x \in \mathbb{Z}$ is PRIME.
Quantifiers range over $\mathbb{Z}$.

PRIMES over $\mathbb{Z}$

I want to say that $x \in \mathbb{Z}$ is PRIME.
Quantifiers range over $\mathbb{Z}$.

$$\text{PRIME}(x) \equiv (x \neq \{0,1\}) \wedge (\forall y,z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

Does this work? Discuss.

PRIMES over $\mathbb{Z}$

I want to say that $x \in \mathbb{Z}$ is PRIME.
Quantifiers range over $\mathbb{Z}$.

$$\mathrm{PRIME}(x) \equiv (x \neq \{0,1\}) \wedge (\forall y, z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

Does this work? Discuss.

$-7 = -1 \times 7$ Its also $-7 \times -1 \times -1 \times 1$. So... not a prime?

PRIMES over $\mathbb{Z}$

I want to say that $x \in \mathbb{Z}$ is PRIME.
Quantifiers range over $\mathbb{Z}$.

$$\mathrm{PRIME}(x) \equiv (x \neq \{0,1\}) \wedge (\forall y, z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

Does this work? Discuss.

$-7 = -1 \times 7$ Its also $-7 \times -1 \times -1 \times 1$. So... not a prime?

NAH, we want -7 to be a prime.

PRIMES over $\mathbb{Z}$ (cont)

$$\mathrm{PRIME}(x) \equiv (x \notin \{0,1\}) \wedge (\forall y, z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

PRIMES over $\mathbb{Z}$ (cont)

$$\mathrm{PRIME}(x) \equiv (x \notin \{0,1\}) \wedge (\forall y, z)[x = yz \to (y = 1) \vee (z = 1)]$$

Why did we make 1 an exception? Because $7 = 1 \times 7$.

PRIMES over $\mathbb{Z}$ (cont)

$$\mathrm{PRIME}(x) \equiv (x \notin \{0,1\}) \wedge (\forall y,z)[x = yz \rightarrow (y=1) \vee (z=1)]$$

Why did we make 1 an exception? Because $7 = 1 \times 7$.

Should we make -1 an exception also?

PRIMES over $\mathbb{Z}$ (cont)

$$\mathrm{PRIME}(x) \equiv (x \notin \{0,1\}) \wedge (\forall y, z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

Why did we make 1 an exception? Because $7 = 1 \times 7$.

Should we make -1 an exception also? Yes.

PRIMES over $\mathbb{Z}$ (cont)

$$\mathrm{PRIME}(x) \equiv (x \notin \{0,1\}) \wedge (\forall y,z)[x = yz \rightarrow (y = 1) \vee (z = 1)]$$

Why did we make 1 an exception? Because $7 = 1 \times 7$.

Should we make -1 an exception also? Yes.

$$\mathrm{PRIME}(x) \equiv (x \notin \{0,1,-1\}) \wedge (\forall y,z)[x = yz \rightarrow (y = \pm 1) \vee (z = \pm 1)]$$

PRIMES over $\mathbb{G}$

Def The **Gaussian Integers** G are numbers of the form

$$\{a + bi : a, b \in \mathbb{Z}\}$$

PRIMES over $\mathbb{G}$

Def The **Gaussian Integers** G are numbers of the form

$$\{a + bi : a, b \in \mathbb{Z}\}$$

We want to define PRIME in G. What will be the exceptional numbers? Why?

PRIMES over $\mathbb{G}$

Def The **Gaussian Integers** G are numbers of the form

$$\{a + bi : a, b \in \mathbb{Z}\}$$

We want to define PRIME in G. What will be the exceptional numbers? Why?
Work in Groups

PRIMES over $\mathbb{G}$

Def The **Gaussian Integers** G are numbers of the form

$$\{a + bi : a, b \in \mathbb{Z}\}$$

We want to define PRIME in G. What will be the exceptional numbers? Why?

Work in Groups

The exceptions are $\{1, -1, i, -i\}$. Why?

PRIMES over $\mathbb{G}$

Def The **Gaussian Integers** G are numbers of the form

$$\{a + bi : a, b \in \mathbb{Z}\}$$

We want to define PRIME in G. What will be the exceptional numbers? Why?

Work in Groups

The exceptions are $\{1, -1, i, -i\}$. Why?

$7 = i \times -i \times 7$.

We don't really want to count the i and $-i$.

Units

Def Let D be some domain. If $x \in D$ then **the mult inverse of x (if it exists)** is the number y such that $xy = 1$.

Units

Def Let D be some domain. If $x \in D$ then **the mult inverse of x (if it exists)** is the number y such that $xy = 1$.

In $\mathbb{N}$ the only number that has a mult inverse is 1.

Units

Def Let D be some domain. If $x \in D$ then **the mult inverse of x (if it exists)** is the number y such that $xy = 1$.

In $\mathbb{N}$ the only number that has a mult inverse is 1.

In $\mathbb{Z}$ the only numbers that has a mult inverses are $1, -1$.

Units

Def Let D be some domain. If $x \in D$ then **the mult inverse of x (if it exists)** is the number y such that $xy = 1$.

In $\mathbb{N}$ the only number that has a mult inverse is 1.

In $\mathbb{Z}$ the only numbers that has a mult inverses are $1, -1$.

In $\mathbb{G}$ the only numbers that has a mult inverses are $1, -1, i, -i$.

Units

Def Let D be some domain. If $x \in D$ then **the mult inverse of x (if it exists)** is the number y such that $xy = 1$.

In $\mathbb{N}$ the only number that has a mult inverse is 1.

In $\mathbb{Z}$ the only numbers that has a mult inverses are $1, -1$.

In $\mathbb{G}$ the only numbers that has a mult inverses are $1, -1, i, -i$.

Def Let D be a domain. The **units of D** are the elements of D that have a multiplicative inverse.

Units

Def Let D be some domain. If $x \in D$ then **the mult inverse of x (if it exists)** is the number y such that $xy = 1$.

In $\mathbb{N}$ the only number that has a mult inverse is 1.

In $\mathbb{Z}$ the only numbers that has a mult inverses are $1, -1$.

In $\mathbb{G}$ the only numbers that has a mult inverses are $1, -1, i, -i$.
Def Let D be a domain. The **units of D** are the elements of D that have a multiplicative inverse.

The Unit are the exceptions. If $x \in D$, u is a unit, and v is its inverse, then
$x = uvx$
We don't want to say x is not prime. u, v should not matter!

Units and Primes

Let D be any domain of numbers.
We will be quantifying over it.

$$\mathrm{UNIT}(x) \equiv (\exists y)[xy = 1]$$

Units and Primes

Let D be any domain of numbers.
We will be quantifying over it.

$$\mathrm{UNIT}(x) \equiv (\exists y)[xy = 1]$$

$$\mathrm{PRIME}(x) \equiv$$

$$(x \neq 0 \wedge \neg\mathrm{UNIT}(x)) \wedge (\forall y, z)[x = yz \rightarrow (\mathrm{UNIT}(y) \vee \mathrm{UNIT}(z)].$$

So Thats why...

1) So thats why 1 is NOT a prime. In any domain D we have
Units, Primes, Composites, 0

So Thats why...

1) So thats why 1 is NOT a prime. In any domain D we have **Units, Primes, Composites, 0**

2) Can we define primes in $\mathbb{Q}$?

So Thats why. . .

1) So thats why 1 is NOT a prime. In any domain D we have **Units, Primes, Composites, 0**

2) Can we define primes in $\mathbb{Q}$? Discuss

So Thats why. . .

1) So thats why 1 is NOT a prime. In any domain D we have
Units, Primes, Composites, 0

2) Can we define primes in $\mathbb{Q}$? Discuss
All elements of $\mathbb{Q}$ are units, so there are no primes.

So Thats why...

1) So thats why 1 is NOT a prime. In any domain D we have
Units, Primes, Composites, 0

2) Can we define primes in $\mathbb{Q}$? Discuss
All elements of $\mathbb{Q}$ are units, so there are no primes.

3) Let $\mathrm{ONEFOUR} = \{n : n \equiv 1 \pmod 4\}$. The only unit is 1.
Note that 9 is PRIME in ONEFOUR since the factorization
$9 = 3 \times 3$ is NOT valid since $3 \notin \mathrm{ONEFOUR}$.

So Thats why...

1) So thats why 1 is NOT a prime. In any domain D we have **Units, Primes, Composites, 0**

2) Can we define primes in $\mathbb{Q}$? Discuss
All elements of $\mathbb{Q}$ are units, so there are no primes.

3) Let $\mathrm{ONEFOUR} = \{n : n \equiv 1 \pmod 4\}$. The only unit is 1.
Note that 9 is PRIME in ONEFOUR since the factorization $9 = 3 \times 3$ is NOT valid since $3 \notin \mathrm{ONEFOUR}$.
What are the primes in $\mathrm{ONEFOUR}$?

So Thats why...

1) So thats why 1 is NOT a prime. In any domain D we have **Units, Primes, Composites, 0**

2) Can we define primes in $\mathbb{Q}$? Discuss
All elements of $\mathbb{Q}$ are units, so there are no primes.

3) Let $\mathrm{ONEFOUR} = \{n : n \equiv 1 \pmod 4\}$. The only unit is 1.
Note that 9 is PRIME in ONEFOUR since the factorization $9 = 3 \times 3$ is NOT valid since $3 \notin \mathrm{ONEFOUR}$.
What are the primes in $\mathrm{ONEFOUR}$? **Work in Groups**

Primes in $\mathrm{ONEFOUR}$

Elements of $\mathrm{ONEFOUR}$: $1, 5, 9, 13, 17, 21, 25$. We stop here.

1: a unit

5: a prime

9: a prime! Note that $3 \notin \mathrm{ONEFOUR}$ so cannot say $9 = 3 \times 3$.

13,17: Primes

21: a prime!

25: 5×5 are first composite.

Primes and Units In Other Domains

Primes and Units In Other Domains

$$\mathbb{D}_d = \{a + b\sqrt{d} \colon a, b \in \mathbb{Z}\}$$

Primes and Units In Other Domains

$\mathbb{D}_d = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$

WORK IN GROUPS

Find all the units of $\mathbb{D}_2$.

Find all the units of $\mathbb{D}_3$.

etc.

Does $\mathbb{D}_2$ Have an Infinite Number of Units

Does $\mathbb{D}_2$ Have an Infinite Number of Units

VOTE

Does $\mathbb{D}_2$ Have an Infinite Number of Units

VOTE

1) $\mathbb{D}_2$ has an infinite number of units.

Does $\mathbb{D}_2$ Have an Infinite Number of Units

VOTE
1) $\mathbb{D}_2$ has an infinite number of units.
2) $\mathbb{D}_2$ has a finite number of unit.

Norm!

Norm!

Let $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. This is called the **conjugate** of $a + b\sqrt{d}$.

Norm!

Let $\overline{a+b\sqrt{d}} = a - b\sqrt{d}$. This is called the **conjugate** of $a+b\sqrt{d}$.
Let $N(a+b\sqrt{d}) = (a+b\sqrt{d})\overline{(a+b\sqrt{d})} = a^2 - db^2d$. Norm!

Norm!

Let $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. This is called the **conjugate** of $a + b\sqrt{d}$.

Let $N(a + b\sqrt{d}) = (a + b\sqrt{d})\overline{(a + b\sqrt{d})} = a^2 - db^2d$. Norm!

Thm $N(\alpha\beta) = N(\alpha)N(\beta)$. HW

Units

Units

Thm If α is a unit then $N(\alpha) = 1$.

Units

Thm If α is a unit then $N(\alpha) = 1$.

α a unit implies $(\exists\beta)[\alpha\beta = 1]$ implies
$N(\alpha\beta) = 1$ implies $N(\alpha)N(\beta) = 1$

Units

Thm If α is a unit then $N(\alpha) = 1$.

α a unit implies $(\exists\beta)[\alpha\beta = 1]$ implies
$N(\alpha\beta) = 1$ implies $N(\alpha)N(\beta) = 1$

Key $N(\alpha)$ and $N(\beta)$ are in $\mathbb{Z}$ so they must be 1 or -1.

Units

Thm If α is a unit then $N(\alpha) = 1$.

α a unit implies $(\exists\beta)[\alpha\beta = 1]$ implies
$N(\alpha\beta) = 1$ implies $N(\alpha)N(\beta) = 1$

Key $N(\alpha)$ and $N(\beta)$ are in $\mathbb{Z}$ so they must be 1 or -1.

Hence $N(\alpha) \in \{-1, 1\}$.

Other Direction

Other Direction

Thm If $N(\alpha) \in \{-1, 1\}$ then α is a unit.
$N(\alpha) = \pm 1$

Other Direction

Thm If $N(\alpha) \in \{-1, 1\}$ then α is a unit.
$N(\alpha) = \pm 1$
$\alpha \overline{alpha} = \pm 1$

Other Direction

Thm If $N(\alpha) \in \{-1, 1\}$ then α is a unit.
$N(\alpha) = \pm 1$
$\alpha\overline{alpha} = \pm 1$
So either $\overline{\alpha}$ or $-\overline{\alpha}$ is the inverse of α.

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

$N(\alpha) = \pm 1$

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

$N(\alpha) = \pm 1$

If $n \in \mathbb{N}$ then
$N(\alpha^n) = N(\alpha)^n = \pm 1.$

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

$N(\alpha) = \pm 1$

If $n \in \mathbb{N}$ then
$N(\alpha^n) = N(\alpha)^n = \pm 1.$

Since α is a unit, $\alpha^{-1} \in \mathbb{D}$.

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

$N(\alpha) = \pm 1$

If $n \in \mathbb{N}$ then
$N(\alpha^n) = N(\alpha)^n = \pm 1$.

Since α is a unit, $\alpha^{-1} \in \mathbb{D}$.

Hence $\alpha^{-n} \in \mathbb{D}$. Easy to show its a unit.

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

$N(\alpha) = \pm 1$

If $n \in \mathbb{N}$ then
$N(\alpha^n) = N(\alpha)^n = \pm 1$.

Since α is a unit, $\alpha^{-1} \in \mathbb{D}$.

Hence $\alpha^{-n} \in \mathbb{D}$. Easy to show its a unit.

This theorem does not guarantee an infinite number of units.

Lemma About Units

Thm If α is a unit then, for all $n \in \mathbb{Z}$, α^n is a unit.

α a unit

$N(\alpha) = \pm 1$

If $n \in \mathbb{N}$ then
$N(\alpha^n) = N(\alpha)^n = \pm 1$.

Since α is a unit, $\alpha^{-1} \in \mathbb{D}$.

Hence $\alpha^{-n} \in \mathbb{D}$. Easy to show its a unit.

This theorem does not guarantee an infinite number of units.
Note that i is a unit in $\mathbb{D}_{-1}$ but $\{i^n \colon n \in \mathbb{Z}\} = \{1, -1, i, -i\}$.

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Need $a, b \in \mathbb{Z}$ such that $a^2 - b^2 d = \pm 1$.

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Need $a, b \in \mathbb{Z}$ such that $a^2 - b^2 d = \pm 1$.

$a^2 - 2b^2 = 1$. Try $b = 0$, $b = 1$, ...

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Need $a, b \in \mathbb{Z}$ such that $a^2 - b^2 d = \pm 1$.

$a^2 - 2b^2 = 1$. Try $b = 0$, $b = 1$, ...
$b = 0$: $(a, b) = (1, 0)$. Thats just 1

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Need $a, b \in \mathbb{Z}$ such that $a^2 - b^2 d = \pm 1$.

$a^2 - 2b^2 = 1$. Try $b = 0$, $b = 1$, ...
$b = 0$: $(a, b) = (1, 0)$. Thats just 1
$b = 1$: $a^2 - 2 = 1$. No Solution.

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Need $a, b \in \mathbb{Z}$ such that $a^2 - b^2 d = \pm 1$.

$a^2 - 2b^2 = 1$. Try $b = 0$, $b = 1$, ...
$b = 0$: $(a, b) = (1, 0)$. Thats just 1
$b = 1$: $a^2 - 2 = 1$. No Solution.
$b = 2$: $a^2 - 8 = 1$. Solution $a = 3$ so $(a, b) = (3, 2)$. $(3 + 2\sqrt{2})$ is a unit.

Back to $\mathbb{D}_2$

Need a unit u in $\mathbb{D}_2$ such that u^n are all different.

Need $a, b \in \mathbb{Z}$ such that $a^2 - b^2 d = \pm 1$.

$a^2 - 2b^2 = 1$. Try $b = 0$, $b = 1$, ...
$b = 0$: $(a, b) = (1, 0)$. Thats just 1
$b = 1$: $a^2 - 2 = 1$. No Solution.
$b = 2$: $a^2 - 8 = 1$. Solution $a = 3$ so $(a, b) = (3, 2)$. $(3 + 2\sqrt{2})$ is a unit.
Infinite number of units: $(3 + 2\sqrt{2})^n$ as $n \in \mathbb{Z}$.