Using Unique Factorization to Proof Numbers Irrational

Recap of Unique Factorization

Thm Every $n \in \mathbb{N}$ factors into primes uniquely.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.
$7b^2 = a^2$.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.

Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.

Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.

$b = p_1^{b_1} \cdots p_L^{b_L}$.

$a = p_1^{a_1} \cdots p_L^{a_L}$.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.

Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.

$b = p_1^{b_1} \cdots p_L^{b_L}$.

$a = p_1^{a_1} \cdots p_L^{a_L}$.

$7b^2 = a^2$, so

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.
Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.
$b = p_1^{b_1} \cdots p_L^{b_L}$.
$a = p_1^{a_1} \cdots p_L^{a_L}$.
$7b^2 = a^2$, so

$$7p_1^{2b_1} \cdots p_L^{2b_L} = p_1^{2a_1} \cdots p_L^{2a_L}$$

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.

Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.

$b = p_1^{b_1} \cdots p_L^{b_L}$.

$a = p_1^{a_1} \cdots p_L^{a_L}$.

$7b^2 = a^2$, so

$$7p_1^{2b_1} \cdots p_L^{2b_L} = p_1^{2a_1} \cdots p_L^{2a_L}$$

How often does 7 appear on LHS? Don't know but its ODD.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.

Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.

$b = p_1^{b_1} \cdots p_L^{b_L}$.

$a = p_1^{a_1} \cdots p_L^{a_L}$.

$7b^2 = a^2$, so

$$7p_1^{2b_1} \cdots p_L^{2b_L} = p_1^{2a_1} \cdots p_L^{2a_L}$$

How often does 7 appear on LHS? Don't know but its ODD.

How often does 7 appear on RHS? Don't know but its EVEN.

Proof that $\sqrt{7} \notin \mathbb{Q}$ Using UF

Assume, BWOC, that $\sqrt{7} = \frac{a}{b}$.

$7b^2 = a^2$.

Factor b and a uniquely.

Let $p_1, \ldots, p_L$ be all of the primes that divide either a or b.

$b = p_1^{b_1} \cdots p_L^{b_L}$.

$a = p_1^{a_1} \cdots p_L^{a_L}$.

$7b^2 = a^2$, so

$$7p_1^{2b_1} \cdots p_L^{2b_L} = p_1^{2a_1} \cdots p_L^{2a_L}$$

How often does 7 appear on LHS? Don't know but its ODD.

How often does 7 appear on RHS? Don't know but its EVEN.

Thats our contradiction!

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.
   PRO of the MOD-proof: Does not rely on any hard theorem.

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.
   PRO of the MOD-proof: Does not rely on any hard theorem.
2. PRO of the UF-proof: Short and does not need the a,b **in lowest terms**.

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.
   PRO of the MOD-proof: Does not rely on any hard theorem.
2. PRO of the UF-proof: Short and does not need the **a, b in lowest terms**.
   CON of the MOD-proof: Has to assume a, b in lowest term and don't see why until the end.

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.
   PRO of the MOD-proof: Does not rely on any hard theorem.
2. PRO of the UF-proof: Short and does not need the ***a*,*b* in lowest terms**.
   CON of the MOD-proof: Has to assume a, b in lowest term and don't see why until the end.

Vote

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.
   PRO of the MOD-proof: Does not rely on any hard theorem.
2. PRO of the UF-proof: Short and does not need the **a,b in lowest terms**.
   CON of the MOD-proof: Has to assume a, b in lowest term and don't see why until the end.

Vote

- Prefer MOD proof.

PROS and CONS of the two Proofs

We have seen two proofs that $\sqrt{7} \notin \mathbb{Q}$.
MOD-proof and UF-proof.

1. CON of the UF-proof: Relies on a hard theorem, Unique Factorization.
   PRO of the MOD-proof: Does not rely on any hard theorem.
2. PRO of the UF-proof: Short and does not need the ***a*,*b* in lowest terms**.
   CON of the MOD-proof: Has to assume a, b in lowest term and don't see why until the end.

Vote

- Prefer MOD proof.
- Prefer UF proof.

Isn't $\mathbb{Z}$ Having Unique Factorization Obvious?

We give an example of a domain that **does not** have unique factorization.

Isn't $\mathbb{Z}$ Having Unique Factorization Obvious?

We give an example of a domain that **does not** have unique factorization.

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

Isn't $\mathbb{Z}$ Having Unique Factorization Obvious?

We give an example of a domain that **does not** have unique factorization.

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

$$6 = 2 \times 3$$

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

Isn't $\mathbb{Z}$ Having Unique Factorization Obvious?

We give an example of a domain that **does not** have unique factorization.

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

$$6 = 2 \times 3$$

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

So it looks like 6 factors two different ways.

Isn't $\mathbb{Z}$ Having Unique Factorization Obvious?

We give an example of a domain that **does not** have unique factorization.

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

$$6 = 2 \times 3$$

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

So it looks like 6 factors two different ways.

But need that $2, 3, 1 + \sqrt{5}, 1 - \sqrt{5}$ are all primes.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm
1) $N(xy) = N(x)N(y)$. Just Algebra.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm
1) $N(xy) = N(x)N(y)$. Just Algebra.
2) $N(x) = 1$ iff x is a unit. Just Algebra.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm
1) $N(xy) = N(x)N(y)$. Just Algebra.
2) $N(x) = 1$ iff x is a unit. Just Algebra.
3) $(\forall x \in D)[N(x) \neq 2]$. Just Algebra.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm
1) $N(xy) = N(x)N(y)$. Just Algebra.
2) $N(x) = 1$ iff x is a unit. Just Algebra.
3) $(\forall x \in D)[N(x) \neq 2]$. Just Algebra.
4) $(\forall x \in D)[N(x) \neq 3]$. Just Algebra.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm
1) $N(xy) = N(x)N(y)$. Just Algebra.
2) $N(x) = 1$ iff x is a unit. Just Algebra.
3) $(\forall x \in D)[N(x) \neq 2]$. Just Algebra.
4) $(\forall x \in D)[N(x) \neq 3]$. Just Algebra.
We use N to prove that $2, 3, 1 + \sqrt{5}, 1 - \sqrt{5}$ are all primes.

Proving Numbers in D are Primes

Recall If D is a domain then there are three kinds of numbers:

1. u is a **unit** if $(\exists u')[uu' = 1]$. Only units of D: $1, -1$.
2. x is a **composite** if $x = yz$ where y, z are not units.
3. x is a **prime** if $x = yz$ implies either y or z is a unit.

Norm $N(a + b\sqrt{5}) = a^2 + 5b^2$.
Thm
1) $N(xy) = N(x)N(y)$. Just Algebra.
2) $N(x) = 1$ iff x is a unit. Just Algebra.
3) $(\forall x \in D)[N(x) \neq 2]$. Just Algebra.
4) $(\forall x \in D)[N(x) \neq 3]$. Just Algebra.
We use N to prove that $2, 3, 1 + \sqrt{5}, 1 - \sqrt{5}$ are all primes.

N is helpful since it maps elements of D (which we don't understand) to $\mathbb{N}$ (which we do understand).

$2, 3$ are Prime

If $2 = xy$ then

2, 3 are Prime

If $2 = xy$ then

$$N(2) = N(xy) = N(x)N(y).$$

$$4 = N(xy) = N(x)N(y).$$

$2, 3$ are Prime

If $2 = xy$ then

$$N(2) = N(xy) = N(x)N(y).$$

$$4 = N(xy) = N(x)N(y).$$

Either
$N(x) = 4$, so $N(y) = 1$: y is a unit OR

$2, 3$ are Prime

If $2 = xy$ then

$$N(2) = N(xy) = N(x)N(y).$$

$$4 = N(xy) = N(x)N(y).$$

Either
$N(x) = 4$, so $N(y) = 1$: y is a unit OR
$N(x) = 2$-not possible OR

$2, 3$ are Prime

If $2 = xy$ then

$$N(2) = N(xy) = N(x)N(y).$$

$$4 = N(xy) = N(x)N(y).$$

Either
$N(x) = 4$, so $N(y) = 1$: y is a unit OR
$N(x) = 2$-not possible OR
$N(x) = 1$ so x is a unit.

$2, 3$ are Prime

If $2 = xy$ then

$$N(2) = N(xy) = N(x)N(y).$$

$$4 = N(xy) = N(x)N(y).$$

Either
$N(x) = 4$, so $N(y) = 1$: y is a unit OR
$N(x) = 2$-not possible OR
$N(x) = 1$ so x is a unit.

3 is prime: Similar to 2.

$1 + \sqrt{5}, 1 - \sqrt{5}$ are Prime

If $1 + \sqrt{5} = xy$ then

$1+\sqrt{5}, 1-\sqrt{5}$ are Prime

If $1+\sqrt{5} = xy$ then
$N(1+\sqrt{5}) = N(xy) = N(x)N(y)$
$6 = N(x)N(y)$.

$1+\sqrt{5}, 1-\sqrt{5}$ are Prime

If $1+\sqrt{5} = xy$ then
$N(1+\sqrt{5}) = N(xy) = N(x)N(y)$
$6 = N(x)N(y)$.
Either
$N(x) = 6$, so $N(y) = 1$, y is a unit OR

$1+\sqrt{5}, 1-\sqrt{5}$ are Prime

If $1+\sqrt{5} = xy$ then
$N(1+\sqrt{5}) = N(xy) = N(x)N(y)$
$6 = N(x)N(y)$.
Either
$N(x) = 6$, so $N(y) = 1$, y is a unit OR
$N(x) = 3$-not possible OR

$1+\sqrt{5}, 1-\sqrt{5}$ are Prime

If $1+\sqrt{5} = xy$ then
$N(1+\sqrt{5}) = N(xy) = N(x)N(y)$
$6 = N(x)N(y)$.
Either
$N(x) = 6$, so $N(y) = 1$, y is a unit OR
$N(x) = 3$-not possible OR
$N(x) = 2$-not poss. OR

$1+\sqrt{5}, 1-\sqrt{5}$ are Prime

If $1+\sqrt{5} = xy$ then
$N(1+\sqrt{5}) = N(xy) = N(x)N(y)$
$6 = N(x)N(y)$.
Either
$N(x) = 6$, so $N(y) = 1$, y is a unit OR
$N(x) = 3$-not possible OR
$N(x) = 2$-not poss. OR
$N(x) = 1$ so x is a unit.

$1+\sqrt{5}, 1-\sqrt{5}$ are Prime

If $1+\sqrt{5} = xy$ then
$N(1+\sqrt{5}) = N(xy) = N(x)N(y)$
$6 = N(x)N(y)$.
Either
$N(x) = 6$, so $N(y) = 1$, y is a unit OR
$N(x) = 3$-not possible OR
$N(x) = 2$-not poss. OR
$N(x) = 1$ so x is a unit.

Proof for $1-\sqrt{5}$ is similar.

Moral of the Story

Moral of the Story

1. Using UF we obtain a different proof that $\sqrt{7} \notin \mathbb{Q}$. Technique works for other proofs of irrationality.

Moral of the Story

1. Using UF we obtain a different proof that $\sqrt{7} \notin \mathbb{Q}$. Technique works for other proofs of irrationality.
2. UF is not obvious. Its false for D so the proof that $\mathbb{Z}$ has UF would need to use properties of $\mathbb{Z}$ that D does not have. We won't be doing that proof, but you now know that it is worthy of proof.