Proposition

Assume \( n \in \mathbb{N} \) has no prime factor \( \leq \sqrt{n} \). Then \( n \) is prime.

Proof.

If \( n = a \cdot b \) with \( a, b > \sqrt{n} \). Then \( a \cdot b > n \).
Proposition

Assume $n \in \mathbb{N}$ has no prime factor $\leq \sqrt{n}$.

Then $n$ is prime.

Proof.

If $n = a \cdot b$ with $a, b > \sqrt{n}$.

Then $a \cdot b > n$. 

\square
Proposition

Assume \( n \in \mathbb{N} \) has no prime factor \( \leq \sqrt{n} \). Then \( n \) is prime.

Proof.

If \( n = a \cdot b \) with \( a, b > \sqrt{n} \). Then \( a \cdot b > n \).
Proposition

Assume \( n \in \mathbb{N} \) has no prime factor \( \leq \sqrt{n} \).
Then \( n \) is prime.

Proof.
If \( n = a \cdot b \) with \( a, b > \sqrt{n} \).
Then \( a \cdot b > n \).
Proposition
Assume $n \in \mathbb{N}$ has no prime factor $\leq \sqrt{n}$.
Then $n$ is prime.

Proof.
If $n = a \cdot b$ with $a, b > \sqrt{n}$.
Then $a \cdot b > n$.  
\qed
Fundamental theorem of Arithmetic

Theorem
Every \( n \in \mathbb{N} \) has a unique factorization as a product of primes.

Proof.
Existence: every \( n \in \mathbb{N} \) has a prime divisor \( p \).

Write \( n = p \cdot n_1 \) and continue by induction.
Fundamental theorem of Arithmetic

**Theorem**

*Every* \( n \in \mathbb{N} \) *has a unique factorization as a product of primes.*

**Proof.**

Existence: every \( n \in \mathbb{N} \) has a prime divisor \( p \).

Write \( n = p \cdot n_1 \) and continue by induction.
Fundamental theorem of Arithmetic

Theorem

Every \( n \in \mathbb{N} \) has a unique factorization as a product of primes.

Proof.

Existence: every \( n \in \mathbb{N} \) has a prime divisor \( p \).

Write \( n = p \cdot n_1 \) and continue by induction.
Fundamental theorem of Arithmetic

Theorem
Every $n \in \mathbb{N}$ has a unique factorization as a product of primes.

Proof.
Existence: every $n \in \mathbb{N}$ has a prime divisor $p$.

Write $n = p \cdot n_1$ and continue by induction. □
Uniqueness: assume \( n \in \mathbb{N} \) is minimal with two factorizations:

Proof.

\[
n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r
\]

\( p_1 \leq p_2 \leq \cdots \leq p_k \) and \( q_1 \leq q_2 \leq \cdots \leq q_r \)

Assume \( p_i \neq q_j \).

\[
n - p_1 q_1 > 0
\]

\( p_1 \) divides \( n - p_1 q_1 \)

\[
n - p_1 q_1 = p_1 m \) so \( q_1 \) divides \( m \)
Uniqueness: assume \( n \in \mathbb{N} \) is minimal with two factorizations:

Proof.

\[
n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r
\]

\( p_1 \leq p_2 \leq \cdots \leq p_k \) and \( q_1 \leq q_2 \leq \cdots \leq q_r \)

Assume \( p_i \neq q_j \).

\[
n - p_1 q_1 > 0
\]

\( p_1 \) divides \( n - p_1 q_1 \)

\[
n - p_1 q_1 = p_1 m \text{ so } q_1 \text{ divides } m
\]
Uniqueness: assume \( n \in \mathbb{N} \) is \textit{minimal} with two factorizations:

Proof.

\[
n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r
\]

\( p_1 \leq p_2 \leq \cdots \leq p_k \) and \( q_1 \leq q_2 \leq \cdots \leq q_r \)

Assume \( p_i \neq q_j \).

\[
n - p_1 q_1 > 0
\]

\( p_1 \) divides \( n - p_1 q_1 \)

\[
n - p_1 q_1 = p_1 m \text{ so } q_1 \text{ divides } m
\]
Uniqueness: assume $n \in \mathbb{N}$ is minimal with two factorizations:

Proof.

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$$

$p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_r$

Assume $p_i \neq q_j$.

$$n = p_1 q_1 > 0$$

$p_1$ divides $n - p_1 q_1$

$$n - p_1 q_1 = p_1 m \text{ so } q_1 \text{ divides } m$$
Uniqueness: assume \( n \in \mathbb{N} \) is minimal with two factorizations:

Proof.

\[ n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r \]

\( p_1 \leq p_2 \leq \cdots \leq p_k \) and \( q_1 \leq q_2 \leq \cdots \leq q_r \)

Assume \( p_i \neq q_j \).

\[ n - p_1 q_1 > 0 \]

\( p_1 \) divides \( n - p_1 q_1 \)

\[ n - p_1 q_1 = p_1 m \] so \( q_1 \) divides \( m \)
Uniqueness: assume $n \in \mathbb{N}$ is minimal with two factorizations:

Proof.

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$$

$p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_r$

Assume $p_i \neq q_j$.

$$n - p_1 q_1 > 0$$

$p_1$ divides $n - p_1 q_1$

$$n - p_1 q_1 = p_1 m$$

so $q_1$ divides $m$.
Uniqueness: assume \( n \in \mathbb{N} \) is minimal with two factorizations:

Proof.

\[
n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r
\]

\( p_1 \leq p_2 \leq \cdots \leq p_k \) and \( q_1 \leq q_2 \leq \cdots \leq q_r \)

Assume \( p_i \neq q_j \).

\[
n - p_1 q_1 > 0
\]

\( p_1 \) divides \( n - p_1 q_1 \)

\[
n - p_1 q_1 = p_1 m \text{ so } q_1 \text{ divides } m
\]
Uniqueness: assume \( n \in \mathbb{N} \) is minimal with two factorizations:

Proof.

\[ n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r \]

\( p_1 \leq p_2 \leq \cdots \leq p_k \) and \( q_1 \leq q_2 \leq \cdots \leq q_r \)

Assume \( p_i \neq q_j \).

\[ n - p_1 q_1 > 0 \]

\( p_1 \) divides \( n - p_1 q_1 \)

\[ n - p_1 q_1 = p_1 m \text{ so } q_1 \text{ divides } m \]
Fundamental theorem of Arithmetic. Continuation

Proof.

\[ p_1 q_1 m_1 = n = p_1 q_1 \]

\[ p_1 q_1 m_1 = p_1 (p_2 p_3 \cdots p_k - q_1) \]

\[ q_1 m_1 = p_2 p_3 \cdots p_k = q_1 \]

\[ q_1 \text{ divides } p_2 p_3 \cdots p_k < n \]

Contradiction to unique factorization.
Proof.

\[ p_1q_1m_1 = n - p_1q_1 \]

\[ p_1q_1m_1 = p_1(p_2p_3 \cdots p_k - q_1) \]

\[ q_1m_1 = p_2p_3 \cdots p_k = q_1 \]

\[ q_1 \text{ divides } p_2p_3 \cdots p_k < n \]

Contradiction to unique factorization.
Fundamental theorem of Arithmetic. Continuation

Proof.

\[ p_1q_1m_1 = n - p_1q_1 \]

\[ p_1q_1m_1 = p_1(p_2p_3\cdots p_k - q_1) \]

\[ q_1m_1 = p_2p_3\cdots p_k = q_1 \]

\[ q_1 \text{ divides } p_2p_3\cdots p_k \leq n \]

Contradiction to unique factorization.
Proof.

\[ p_1q_1m_1 = n - p_1q_1 \]

\[ p_1q_1m_1 = p_1(p_2p_3 \cdots p_k - q_1) \]

\[ q_1m_1 = p_2p_3 \cdots p_k - q_1 \]

\( q_1 \) divides \( p_2p_3 \cdots p_k \leq n \)

Contradiction to unique factorization.
Fundamental theorem of Arithmetic. Continuation

Proof.

\[ p_1q_1m_1 = n - p_1q_1 \]
\[ p_1q_1m_1 = p_1(p_2p_3 \cdots p_k - q_1) \]
\[ q_1m_1 = p_2p_3 \cdots p_k - q_1 \]
\[ q_1 \text{ divides } p_2p_3 \cdots p_k < n \]

Contradiction to unique factorization.
Fundamental theorem of Arithmetic. Continuation

Proof.

\[ p_1q_1m_1 = n - p_1q_1 \]

\[ p_1q_1m_1 = p_1(p_2p_3 \cdots p_k - q_1) \]

\[ q_1m_1 = p_2p_3 \cdots p_k - q_1 \]

\[ q_1 \text{ divides } p_2p_3 \cdots p_k < n \]

Contradiction to unique factorization.
Exercise

Check the details of the following proof that $\mathbb{Q}$ is countable.

$m = p_1^{e_1} \cdots p_r^{e_r}$ and $n = q_1^{f_1} \cdots q_k^{f_k}$

define

$$T \left( \frac{m}{n} \right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1 - 1} q_2^{2f_2 - 1} \cdots q_k^{2f_k - 1}$$

a) Find $T(123456)$.

b) Which $x \in \mathbb{Q}$ gives $T(x) = 1221$.

c) Prove that $T$ is one-to-one and onto.

d) What does it mean to be countable?
Exercise

Check the details of the following proof that \( \mathbb{Q} \) is countable.

\[
m = p_1^{e_1} \cdots p_r^{e_r} \text{ and } n = q_1^{f_1} \cdots q_k^{f_k}
\]

define

\[
T \left( \frac{m}{n} \right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1 - 1} q_2^{2f_2 - 1} \cdots q_k^{2f_k - 1}
\]

a) Find \( T(123456) \).

b) Which \( x \in \mathbb{Q} \) gives \( T(x) = 1221 \).

c) Prove that \( T \) is one-to-one and onto.

d) What does it mean to be countable?
Exercise

Check the details of the following proof that \( \mathbb{Q} \) is countable.

\[
m = p_1^{e_1} \cdots p_r^{e_r} \text{ and } n = q_1^{f_1} \cdots q_k^{f_k}
\]

define

\[
T \left( \frac{m}{n} \right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1 - 1} q_2^{2f_2 - 1} \cdots q_k^{2f_k - 1}
\]

a) Find \( T(123456) \).
b) Which \( x \in \mathbb{Q} \) gives \( T(x) = 1221 \).
c) Prove that \( T \) is one-to-one and onto.
d) What does it mean to be countable?
Exercise

Check the details of the following proof that \( \mathbb{Q} \) is countable.

\[
m = p_1^{e_1} \cdots p_r^{e_r} \text{ and } n = q_1^{f_1} \cdots q_k^{f_k}
\]

define

\[
T \left( \frac{m}{n} \right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1-1} q_2^{2f_2-1} \cdots q_k^{2f_k-1}
\]

a) Find \( T(123456) \).

b) Which \( x \in \mathbb{Q} \) gives \( T(x) = 1221 \).

c) Prove that \( T \) is one-to-one and onto.

d) What does it mean to be countable?
Exercise

Check the details of the following proof that $\mathbb{Q}$ is countable.

$$m = p_1^{e_1} \cdots p_r^{e_r} \text{ and } n = q_1^{f_1} \cdots q_k^{f_k}$$

define

$$T\left(\frac{m}{n}\right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1-1} q_2^{2f_2-1} \cdots q_k^{2f_k-1}$$

a) Find $T(123456)$.
b) Which $x \in \mathbb{Q}$ gives $T(x) = 1221$.
c) Prove that $T$ is one-to-one and onto.
d) What does it mean to be countable?
Exercise

Check the details of the following proof that \( \mathbb{Q} \) is countable.

\[ m = p_1^{e_1} \cdots p_r^{e_r} \text{ and } n = q_1^{f_1} \cdots q_k^{f_k} \]

define

\[ T \left( \frac{m}{n} \right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1-1} q_2^{2f_2-1} \cdots q_k^{2f_k-1} \]

a) Find \( T(123456) \).

b) Which \( x \in \mathbb{Q} \) gives \( T(x) = 1221 \).

c) Prove that \( T \) is one-to-one and onto.

d) What does it mean to be countable?
Exercise

Check the details of the following proof that \( \mathbb{Q} \) is countable.

\[
m = p_1^{e_1} \cdots p_r^{e_r} \text{ and } n = q_1^{f_1} \cdots q_k^{f_k}
\]

Define

\[
T \left( \frac{m}{n} \right) = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} q_1^{2f_1 - 1} q_2^{2f_2 - 1} \cdots q_k^{2f_k - 1}
\]

a) Find \( T(123456) \).

b) Which \( x \in \mathbb{Q} \) gives \( T(x) = 1221 \).

c) Prove that \( T \) is one-to-one and onto.

d) What does it mean to be countable?