Math 3110 Lecture 12

Greg Oman

University of Colorado
Colorado Springs

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

Let p be a prime, let a and b be integers, and assume that $p|ab$.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

Let p be a prime, let a and b be integers, and assume that $p|ab$. From your homework, either $p|a$ or p and a are relatively prime.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

Let p be a prime, let a and b be integers, and assume that $p|ab$. From your homework, either $p|a$ or p and a are relatively prime. If $p|a$, we are done.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

Let p be a prime, let a and b be integers, and assume that $p|ab$. From your homework, either $p|a$ or p and a are relatively prime. If $p|a$, we are done. So assume that $p \nmid a$.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

Let p be a prime, let a and b be integers, and assume that $p|ab$. From your homework, either $p|a$ or p and a are relatively prime. If $p|a$, we are done. So assume that $p \nmid a$. Then p and a are relatively prime, and so by Euclid's Lemma, $p|b$.

Finishing the FTA

We are almost ready to prove the so-called Fundamental Theorem of Arithmetic, but first we need a couple more lemmas. First, let's recall Euclid's Lemma (I proved this for you a few weeks back):

Theorem (Euclid's Lemma)

Let $x, y, z \in \mathbb{Z}$, and suppose that $x|yz$. If x and y are relatively prime, then $x|z$.

Corollary

Let p be a prime number and let a and b be integers. If $p|ab$, then either $p|a$ or $p|b$.

Proof.

Let p be a prime, let a and b be integers, and assume that $p|ab$. From your homework, either $p|a$ or p and a are relatively prime. If $p|a$, we are done. So assume that $p \nmid a$. Then p and a are relatively prime, and so by Euclid's Lemma, $p|b$. This concludes the proof. $\square$

Finishing the FTA

Corollary

Let p be a prime.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n. Now let $a_1, \ldots, a_{n+1}$ be integers and assume that $p|a_1 \cdots a_{n+1}$.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n. Now let $a_1, \ldots, a_{n+1}$ be integers and assume that $p|a_1 \cdots a_{n+1}$. Then $p|(a_1 \cdots a_n) \cdot a_{n+1}$.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n. Now let $a_1, \ldots, a_{n+1}$ be integers and assume that $p|a_1 \cdots a_{n+1}$. Then $p|(a_1 \cdots a_n) \cdot a_{n+1}$. By the first corollary on the previous slide, either $p|a_1 \cdots a_n$ or $p|a_{n+1}$.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n. Now let $a_1, \ldots, a_{n+1}$ be integers and assume that $p|a_1 \cdots a_{n+1}$. Then $p|(a_1 \cdots a_n) \cdot a_{n+1}$. By the first corollary on the previous slide, either $p|a_1 \cdots a_n$ or $p|a_{n+1}$. In the latter case, we are done.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n. Now let $a_1, \ldots, a_{n+1}$ be integers and assume that $p|a_1 \cdots a_{n+1}$. Then $p|(a_1 \cdots a_n) \cdot a_{n+1}$. By the first corollary on the previous slide, either $p|a_1 \cdots a_n$ or $p|a_{n+1}$. In the latter case, we are done. So suppose that $p|a_1 \cdots a_n$.

Finishing the FTA

Corollary

Let p be a prime. Then for every positive integer n: if $a_1, \ldots, a_n$ are integers and $p|a_1 \cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof.

Let p be a prime.

(i) (base case) Assume that a_1 is an integer and that $p|a_1$. Then $p|a_1$ and we are done.

(ii) (inductive step) Let n be an arbitrary positive integer, and assume that claim is true for n. Now let $a_1, \ldots, a_{n+1}$ be integers and assume that $p|a_1 \cdots a_{n+1}$. Then $p|(a_1 \cdots a_n) \cdot a_{n+1}$. By the first corollary on the previous slide, either $p|a_1 \cdots a_n$ or $p|a_{n+1}$. In the latter case, we are done. So suppose that $p|a_1 \cdots a_n$. Then by the inductive hypothesis, $p|a_i$ for some i, $1 \leq i \leq n$, and we are done. $\square$

Finishing the FTA

Corollary

If p and $q_1, \ldots, q_n$ are primes such that $p | q_1 \cdots q_n$, then $p = q_i$ for some i, $1 \leq i \leq n$.

Finishing the FTA

Corollary

If p and $q_1, \ldots, q_n$ are primes such that $p|q_1 \cdots q_n$, then $p = q_i$ for some i, $1 \leq i \leq n$.

Proof.

Let p and $q_1, \ldots, q_n$ be primes and assume that $p|q_1 \cdots q_n$.

Finishing the FTA

Corollary

If p and $q_1, \ldots, q_n$ are primes such that $p|q_1 \cdots q_n$, then $p = q_i$ for some i, $1 \leq i \leq n$.

Proof.

Let p and $q_1, \ldots, q_n$ be primes and assume that $p|q_1 \cdots q_n$. Then by the previous corollary, $p|q_i$ for some i with $1 \leq i \leq n$.

Finishing the FTA

Corollary

If p and $q_1, \ldots, q_n$ are primes such that $p|q_1 \cdots q_n$, then $p = q_i$ for some i, $1 \leq i \leq n$.

Proof.

Let p and $q_1, \ldots, q_n$ be primes and assume that $p|q_1 \cdots q_n$. Then by the previous corollary, $p|q_i$ for some i with $1 \leq i \leq n$. But now p is a positive factor of the prime q_i which is NOT one. It follows that $p = q_i$, by def. of 'prime.' $\square$

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$. We must show that $x \in \{q_1, \ldots, q_m\}$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$. We must show that $x \in \{q_1, \ldots, q_m\}$. We have $x = p_i$ for some i, $1 \leq i \leq n$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$. We must show that $x \in \{q_1, \ldots, q_m\}$. We have $x = p_i$ for some i, $1 \leq i \leq n$. Since $p_1 \cdots p_n = q_1 \cdots q_m$, it follows that $p_i | q_1 \cdots q_m$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ and $q_1, \ldots, q_m$ are primes such that $p_1 \cdots p_n = q_1 \cdots q_m$. Then $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$. We must show that $x \in \{q_1, \ldots, q_m\}$. We have $x = p_i$ for some i, $1 \leq i \leq n$. Since $p_1 \cdots p_n = q_1 \cdots q_m$, it follows that $p_i | q_1 \cdots q_m$. By the previous corollary, $x = p_i = q_j$ for some j, $1 \leq j \leq m$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ *and* $q_1, \ldots, q_m$ *are primes such that* $p_1 \cdots p_n = q_1 \cdots q_m$. *Then* $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$. We must show that $x \in \{q_1, \ldots, q_m\}$. We have $x = p_i$ for some i, $1 \leq i \leq n$. Since $p_1 \cdots p_n = q_1 \cdots q_m$, it follows that $p_i | q_1 \cdots q_m$. By the previous corollary, $x = p_i = q_j$ for some j, $1 \leq j \leq m$. This shows that $x \in \{q_1, \ldots, q_m\}$, and we have shown that $\{p_1, \ldots, p_n\} \subseteq \{q_1, \ldots, q_m\}$.

Finishing the FTA

Corollary

Suppose that $p_1, \ldots, p_n$ and $q_1, \ldots, q_m$ are primes such that $p_1 \cdots p_n = q_1 \cdots q_m$. Then $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_m\}$.

Proof.

Let the p_i, q_j be as stated and suppose that $p_1 \cdots p_n = q_1 \cdots q_m$. Now take any $x \in \{p_1, \ldots, p_n\}$. We must show that $x \in \{q_1, \ldots, q_m\}$. We have $x = p_i$ for some i, $1 \leq i \leq n$. Since $p_1 \cdots p_n = q_1 \cdots q_m$, it follows that $p_i | q_1 \cdots q_m$. By the previous corollary, $x = p_i = q_j$ for some j, $1 \leq j \leq m$. This shows that $x \in \{q_1, \ldots, q_m\}$, and we have shown that $\{p_1, \ldots, p_n\} \subseteq \{q_1, \ldots, q_m\}$. A symmetric argument shows that $\{q_1, \ldots, q_m\} \subseteq \{p_1, \ldots, p_n\}$, and the proof is complete. $\square$

Finishing the FTA

We are almost ready to present the FTA.

Finishing the FTA

We are almost ready to present the FTA. First, a final definition.

Finishing the FTA

We are almost ready to present the FTA. First, a final definition.

Definition

Let $p_1 < p_2 \cdots < p_k$ be prime numbers, and let $n_1, \ldots, n_k$ be positive integers.

Finishing the FTA

We are almost ready to present the FTA. First, a final definition.

Definition

Let $p_1 < p_2 \cdots < p_k$ be prime numbers, and let $n_1, \ldots, n_k$ be positive integers. Then we say that the product $p_1^{n_1} \cdots p_k^{n_k}$ is a **product of primes in canonical form**.

Finishing the FTA

We are almost ready to present the FTA. First, a final definition.

Definition

Let $p_1 < p_2 \cdots < p_k$ be prime numbers, and let $n_1, \ldots, n_k$ be positive integers. Then we say that the product $p_1^{n_1} \cdots p_k^{n_k}$ is a **product of primes in canonical form**.

Example

$2^3 \cdot 5^6 \cdot 3^4$ is NOT a product of primes in canonical form, but $2^3 \cdot 3^4 \cdot 5^6$ is.

Finishing the FTA

We are almost ready to present the FTA. First, a final definition.

Definition

Let $p_1 < p_2 \cdots < p_k$ be prime numbers, and let $n_1, \ldots, n_k$ be positive integers. Then we say that the product $p_1^{n_1} \cdots p_k^{n_k}$ is a **product of primes in canonical form**.

Example

$2^3 \cdot 5^6 \cdot 3^4$ is NOT a product of primes in canonical form, but $2^3 \cdot 3^4 \cdot 5^6$ is.

Example

Write $3 \cdot 7 \cdot 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2$ as a product of primes in canonical form.

Finishing the FTA

We are almost ready to present the FTA. First, a final definition.

Definition

Let $p_1 < p_2 \cdots < p_k$ be prime numbers, and let $n_1, \ldots, n_k$ be positive integers. Then we say that the product $p_1^{n_1} \cdots p_k^{n_k}$ is a **product of primes in canonical form**.

Example

$2^3 \cdot 5^6 \cdot 3^4$ is NOT a product of primes in canonical form, but $2^3 \cdot 3^4 \cdot 5^6$ is.

Example

Write $3 \cdot 7 \cdot 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2$ as a product of primes in canonical form.

Solution.

$2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1$. □

Finishing the FTA

From the previous example, it should be clear that, from a given product of primes, we can rewrite it so that it is in canonical form.

Finishing the FTA

From the previous example, it should be clear that, from a given product of primes, we can rewrite it so that it is in canonical form. We now state and prove the Fundamental Theorem of Arithmetic.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $m > 1$ can be written uniquely as a product of primes in canonical form.

Finishing the FTA

From the previous example, it should be clear that, from a given product of primes, we can rewrite it so that it is in canonical form. We now state and prove the Fundamental Theorem of Arithmetic.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $m > 1$ can be written uniquely as a product of primes in canonical form. In other words, if $m > 1$ is an integer, then there exist primes $p_1 < \cdots < p_k$ and positive integers $n_1, \ldots, n_k$ such that $m = p_1^{n_1} \cdots p_k^{n_k}$.

Finishing the FTA

From the previous example, it should be clear that, from a given product of primes, we can rewrite it so that it is in canonical form. We now state and prove the Fundamental Theorem of Arithmetic.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $m > 1$ can be written uniquely as a product of primes in canonical form. In other words, if $m > 1$ is an integer, then there exist primes $p_1 < \cdots < p_k$ and positive integers $n_1, \ldots, n_k$ such that $m = p_1^{n_1} \cdots p_k^{n_k}$. Moreover, if $q_1 < \cdots < q_r$ are primes and $m = q_1^{a_1} \cdots q_r^{a_r}$, with each a_i a positive integer, then $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$.

Finishing the FTA

From the previous example, it should be clear that, from a given product of primes, we can rewrite it so that it is in canonical form. We now state and prove the Fundamental Theorem of Arithmetic.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $m > 1$ can be written uniquely as a product of primes in canonical form. In other words, if $m > 1$ is an integer, then there exist primes $p_1 < \cdots < p_k$ and positive integers $n_1, \ldots, n_k$ such that $m = p_1^{n_1} \cdots p_k^{n_k}$. Moreover, if $q_1 < \cdots < q_r$ are primes and $m = q_1^{a_1} \cdots q_r^{a_r}$, with each a_i a positive integer, then $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$.

Proof.

Recall last week that we showed that every integer $m \geq 2$ is either prime or the product of two or more primes, that is, $m = p_1 \cdots p_n$ for some integer $n \geq 1$ and prime numbers $p_1, \ldots, p_n$.

Finishing the FTA

From the previous example, it should be clear that, from a given product of primes, we can rewrite it so that it is in canonical form. We now state and prove the Fundamental Theorem of Arithmetic.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $m > 1$ can be written uniquely as a product of primes in canonical form. In other words, if $m > 1$ is an integer, then there exist primes $p_1 < \cdots < p_k$ and positive integers $n_1, \ldots, n_k$ such that $m = p_1^{n_1} \cdots p_k^{n_k}$. Moreover, if $q_1 < \cdots < q_r$ are primes and $m = q_1^{a_1} \cdots q_r^{a_r}$, with each a_i a positive integer, then $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$.

Proof.

Recall last week that we showed that every integer $m \geq 2$ is either prime or the product of two or more primes, that is, $m = p_1 \cdots p_n$ for some integer $n \geq 1$ and prime numbers $p_1, \ldots, p_n$. By the preceding discussing, this enables us to write m as a product of primes in canonical form. □

Finishing the FTA

Proof.

So now it remains only to prove uniqueness.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?).

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$. So we now have $m = p_1^{n_1} \cdots p_k^{n_k} = p_1^{a_1} \cdots p_k^{a_k}$.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$. So we now have $m = p_1^{n_1} \cdots p_k^{n_k} = p_1^{a_1} \cdots p_k^{a_k}$. I will show you that $n_1 = a_1$;

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$. So we now have $m = p_1^{n_1} \cdots p_k^{n_k} = p_1^{a_1} \cdots p_k^{a_k}$. I will show you that $n_1 = a_1$; that the rest of the powers are equal follows analogously.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$. So we now have $m = p_1^{n_1} \cdots p_k^{n_k} = p_1^{a_1} \cdots p_k^{a_k}$. I will show you that $n_1 = a_1$; that the rest of the powers are equal follows analogously. Suppose by way of contradiction that $n_1 \neq a_1$; without loss of generality, $n_1 < a_1$.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$. So we now have $m = p_1^{n_1} \cdots p_k^{n_k} = p_1^{a_1} \cdots p_k^{a_k}$. I will show you that $n_1 = a_1$; that the rest of the powers are equal follows analogously. Suppose by way of contradiction that $n_1 \neq a_1$; without loss of generality, $n_1 < a_1$. Divide both sides of the above equation by $p_1^{n_1}$ to get $p_2^{n_2} \cdots p_k^{n_k} = p_1^{a_1 - n_1} \cdots p_k^{n_k}$.

Finishing the FTA

Proof.

So now it remains only to prove uniqueness. Suppose that $m > 1$ and that we have $m = p_1^{n_1} \cdots p_k^{n_k} = q_1^{a_1} \cdots q_r^{a_r}$, where p_i, q_j are primes, and n_i, a_j are positive integers. We must show that $k = r$, $p_i = q_i$, and $n_i = a_i$ for $1 \leq i \leq k$. From an earlier lemma, we see that $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_r\}$. It follows that $k = r$ and that $p_i = q_i$ for $1 \leq i \leq k$ (WHY?). It remains only to show that $n_i = a_i$ for $1 \leq i \leq r$. So we now have $m = p_1^{n_1} \cdots p_k^{n_k} = p_1^{a_1} \cdots p_k^{a_k}$. I will show you that $n_1 = a_1$; that the rest of the powers are equal follows analogously. Suppose by way of contradiction that $n_1 \neq a_1$; without loss of generality, $n_1 < a_1$. Divide both sides of the above equation by $p_1^{n_1}$ to get $p_2^{n_2} \cdots p_k^{n_k} = p_1^{a_1 - n_1} \cdots p_k^{n_k}$. But then we get $\{p_2, \ldots, p_k\} = \{p_1, \ldots, p_k\}$, a contradiction. □

Finishing the FTA

Example

Let m and n be non-negative integers.

Finishing the FTA

Example

Let m and n be non-negative integers. Prove that if $3^m = 5^n$, then $m = n = 0$.