Fundamental Theorem of Arithmetic

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

Table of Contents

Fundamental Theorem of Arithmetic

Theorem

Every positive integer n can be written as a product of prime integers

$$n = p_1 p_2 p_3 \cdots p_k$$

which is unique up to order.

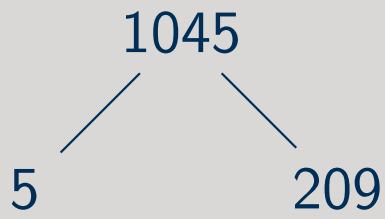
Fundamental Theorem of Arithmetic

Example

1045

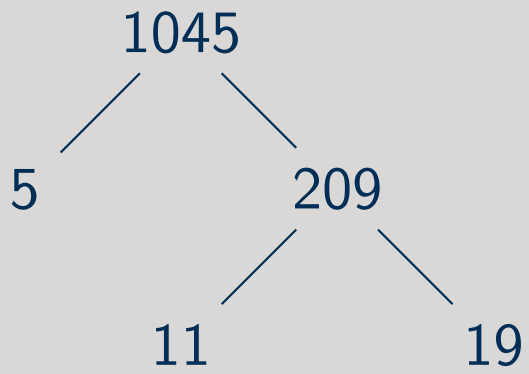
Fundamental Theorem of Arithmetic

Example



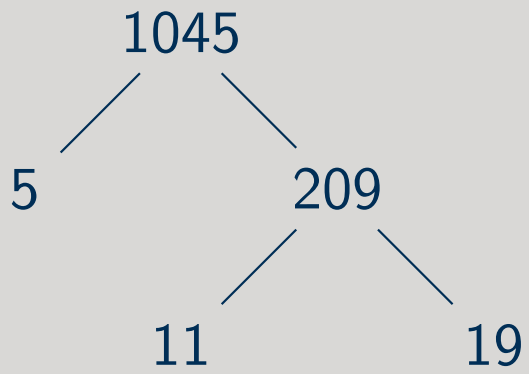
Fundamental Theorem of Arithmetic

Example



Fundamental Theorem of Arithmetic

Example



$$1045 = 5 \cdot 11 \cdot 19$$

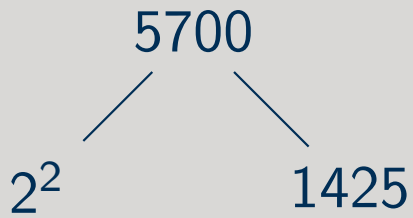
Fundamental Theorem of Arithmetic

Example

5700

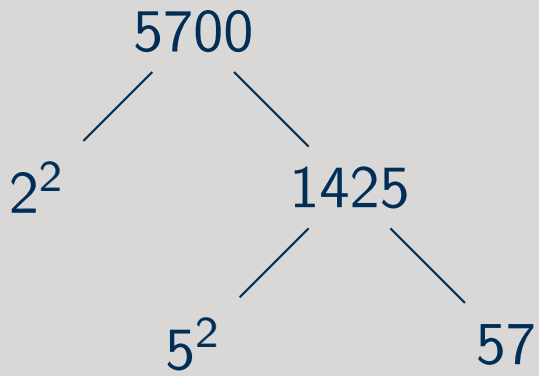
Fundamental Theorem of Arithmetic

Example



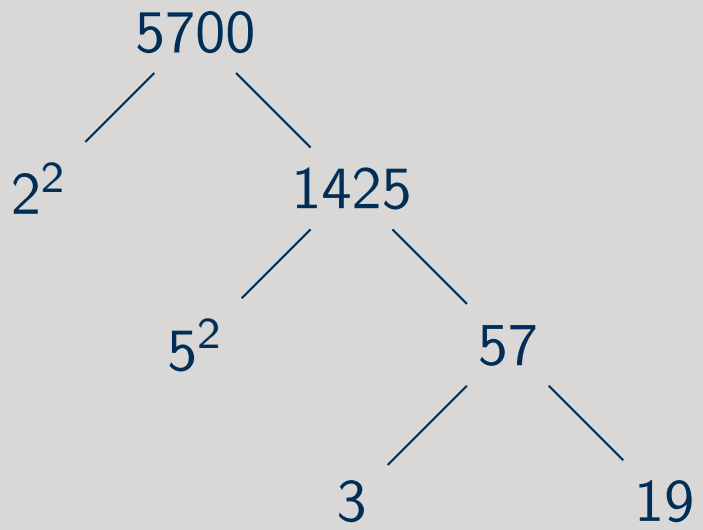
Fundamental Theorem of Arithmetic

Example



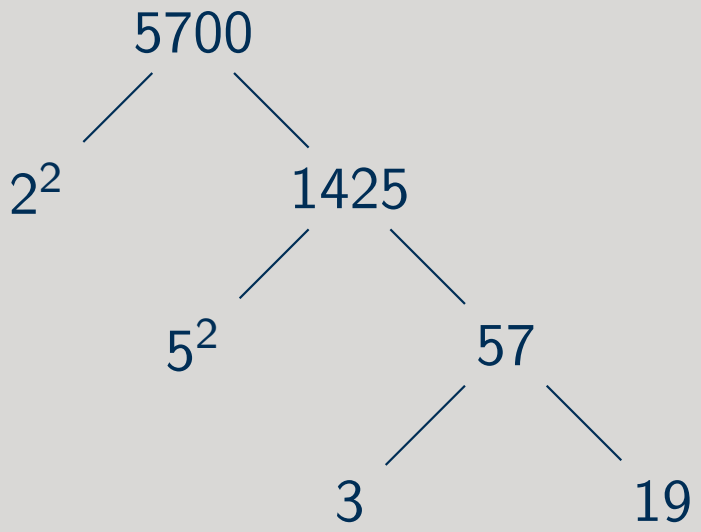
Fundamental Theorem of Arithmetic

Example



Fundamental Theorem of Arithmetic

Example



$$5700 = 2^2 \cdot 5^2 \cdot 3 \cdot 19$$

Fundamental Theorem of Arithmetic

Observations

- Factors less than the square root of n

Fundamental Theorem of Arithmetic

Observations

- Factors less than the square root of n
- Only need to look for prime factors

Fundamental Theorem of Arithmetic

Observations

- Factors less than the square root of n
- Only need to look for prime factors
- Factors of $2, 4, 8 \ldots$

Fundamental Theorem of Arithmetic

Observations

- Factors less than the square root of n
- Only need to look for prime factors
- Factors of $2, 4, 8 \ldots$
- Factors of $3, 6$ and 9

Fundamental Theorem of Arithmetic

Observations

- Factors less than the square root of n
- Only need to look for prime factors
- Factors of $2, 4, 8 \ldots$
- Factors of $3, 6$ and 9
- Factors of $5, 25, 125, \ldots$

Path to the Fundamental Theorem

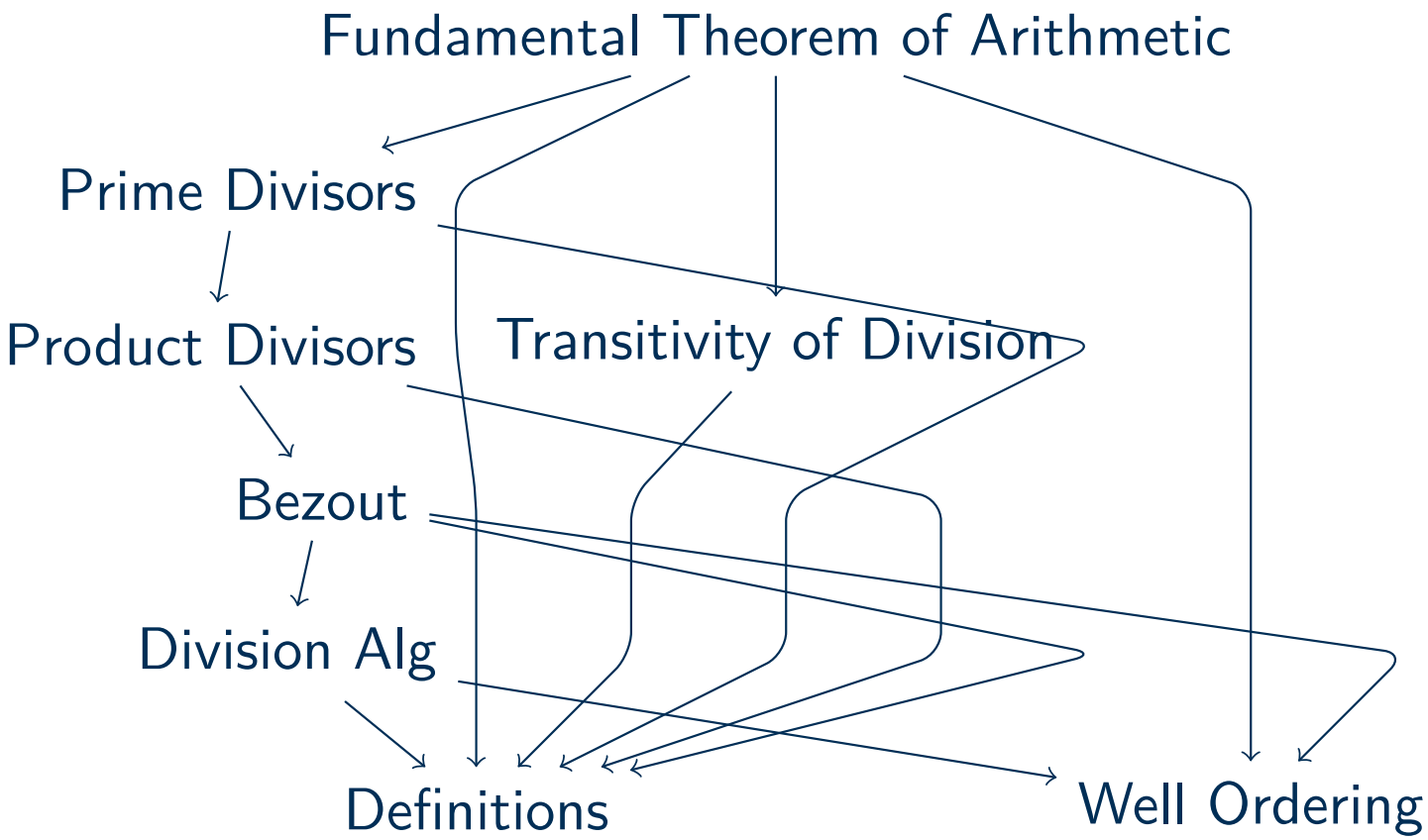


Table of Contents

Divisibility

Definition

Given two integers a and b we say b divides a if there exists a unique q such that $a = qb$. For example 4 divides 36 because $36 = 9 \cdot 4$.

Greatest Common Divisor

Definition

The greatest common divisor of two integers a and b is the largest positive integer d which divides both a and b. For example $17 = \gcd(85, 102)$ since $85 = 5 \cdot 17$ and $102 = 6 \cdot 17$.

Prime and Composite Numbers

Definition

A positive integer is prime if it has exactly two divisors one and its self, otherwise it is composite.

Well Ordering Principle

Axiom

Every non-empty set of non-negative integers has a least element.

Table of Contents

Transitivity

Lemma

Given three integers a, b, c if a divides b and b divides c, then a divides c. For example 3 divides 6 since $6 = 2 \cdot 3$ and 6 divides 42 since $42 = 7 \cdot 6$, so 3 divides 42 since

$$42 = 7 \cdot 6 = 7 \cdot (2 \cdot 3).$$

Division Algorithm

Theorem

Given integers a, b with $b \neq 0$, there exists a unique quotient q and remainder r such that

$$a = q \cdot b + r$$

with $0 \leq r < |b|$. For example if $a = 17$ and $b = 7$ then we can write $17 = 2 \cdot 7 + 3$.

Bezout's Lemma

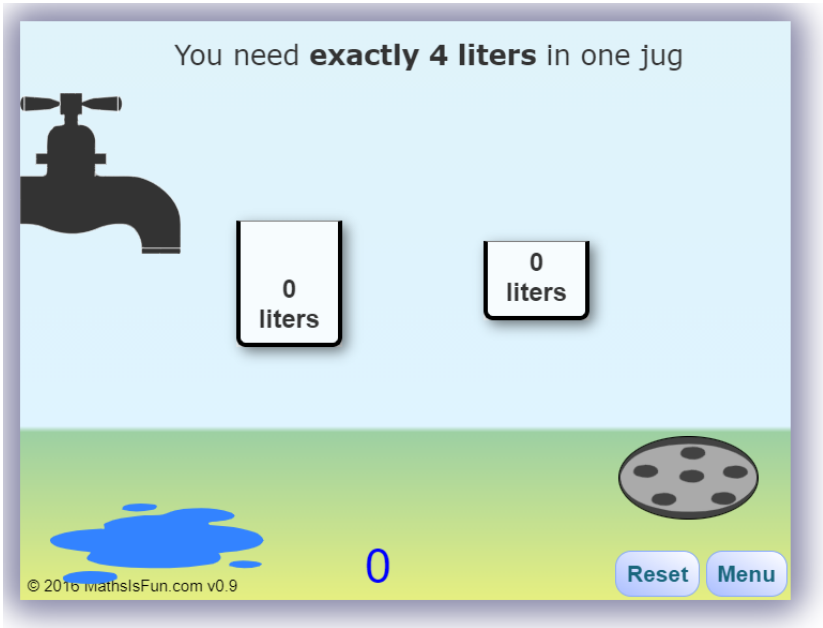
Lemma

Given integers a, b with greatest common divisor d, there exists integers x, y such that

$$d = ax + by.$$

Furthermore, d is the least positive integer for which this works. For example, if $a = 17$ and $b = 7$ the greatest common divisor is 1 and we can write $1 = 17(-2) + 7(5)$.

Saving the World with Math



https://www.mathsisfun.com/games/jugs-puzzle.html

Product Divisors

Lemma

If a, b, c are integers such that c divides ab and $\gcd(a, c) = 1$, then c divides b.

Prime Divisors

Lemma

If a, b, p are integers such that p divides ab and p is prime, then p divides at least one of a or b.

Table of Contents

Steps to the Fundamental Theorem

- All positive integers are a product of primes.

Steps to the Fundamental Theorem

- All positive integers are a product of primes.
- The product of primes is unique up to order.

Fundamental Theorem of Arithmetic

Observations

- Factors less than the square root of n
- Only need to look for prime factors
- Factors of $2, 4, 8 \ldots$
- Factors of $3, 6$ and 9
- Factors of $5, 25, 125, \ldots$

Fundamental Theorem of Arithmetic

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES