Math 322 Notes on integers and divisibility

Zinovy Reichstein

September 13, 2016
We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer.
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. 
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$.
- $a$ evenly divides $b$.
- $b$ is divisible by $a$.
- $b$ is a multiple of $a$. 

We say that an integer $n \geq 2$ is a prime if $n$ is not divisible by any positive integer, other than 1 and $n$ itself. Integers $n \geq 2$ that are not prime are called composite. For example, 2, 3, 5, 7, 11, 13 are all primes, but 6 = 2·3 and 9 = 3·3 are composite.
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$, 

Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$,
- $a$ evenly divides $b$,
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$,
- $a$ evenly divides $b$,
- $b$ is divisible by $a$,
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$,
- $a$ evenly divides $b$,
- $b$ is divisible by $a$,
- $b$ is a multiple of $a$. 
Divisibility

We say that an integer \( a \) divides another integer \( b \), if \( b/a \) is an integer. That is, \( b = an \) for some integer \( n \). Here we assume that \( a \neq 0 \), but allow \( b \) to be an arbitrary integer.

The following expressions all mean the same thing:

- \( a \) divides \( b \),
- \( a \) evenly divides \( b \),
- \( b \) is divisible by \( a \),
- \( b \) is a multiple of \( a \).

We say that an integer \( n \) is a prime if \( n \geq 2 \) and \( n \) is not divisible by any positive integer, other than 1 and \( n \) itself.
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$,
- $a$ evenly divides $b$,
- $b$ is divisible by $a$,
- $b$ is a multiple of $a$.

We say that an integer $n$ is a prime if $n \geq 2$ and $n$ is not divisible by any positive integer, other than 1 and $n$ itself. Integers $n \geq 2$ that are not prime are called composite.
Divisibility

We say that an integer $a$ divides another integer $b$, if $b/a$ is an integer. That is, $b = an$ for some integer $n$. Here we assume that $a \neq 0$, but allow $b$ to be an arbitrary integer.

The following expressions all mean the same thing:

- $a$ divides $b$,
- $a$ evenly divides $b$,
- $b$ is divisible by $a$,
- $b$ is a multiple of $a$.

We say that an integer $n$ is a prime if $n \geq 2$ and $n$ is not divisible by any positive integer, other than 1 and $n$ itself. Integers $n \geq 2$ that are not prime are called composite.

For example, 2, 3, 5, 7, 11, 13 are all primes, but $6 = 2 \cdot 3$ and $9 = 3 \cdot 3$ are composite.
Theorem: Every integer $n \geq 2$ is either a prime or a product of two or more primes.
Theorem: Every integer \( n \geq 2 \) is either a prime or a product of two or more primes.

This is readily proved by strong induction on \( n \). (Check!)
Theorem: Every integer $n \geq 2$ is either a prime or a product of two or more primes.

This is readily proved by strong induction on $n$. (Check!)

Note however that inductive proof does not give an algorithm for writing a given integer as a product of primes.
Theorem: Every integer $n \geq 2$ is either a prime or a product of two or more primes.

This is readily proved by strong induction on $n$. (Check!)

Note however that inductive proof does not give an algorithm for writing a given integer as a product of primes.

Such algorithms are in short supply and are of crucial importance in cryptography.
Euclid of Alexandria, approx. 300 BC

The theorem on the previous slide is stated and proved in Euclid's "Elements," arguably the most influential mathematics book ever written. This book was used as a textbook since 300 B.C. into the 20th century.
Euclid of Alexandria, approx. 300 BC

The theorem on the previous slide
Euclid of Alexandria, approx. 300 BC

The theorem on the previous slide is stated and proved in Euclid’s “Elements”,

Math 322, Notes on integers and divisibility
The theorem on the previous slide is stated and proved in Euclid’s “Elements”, arguably the most influential mathematics book ever written. This book was used...
Euclid of Alexandria, approx. 300 BC

The theorem on the previous slide is stated and proved in Euclid’s “Elements”, arguably the most influential mathematics book ever written. This book was used as a textbook since 300 B.C. into the 20th century.
The division algorithm

Theorem: Let \( a \geq 1 \) be an integer.
The division algorithm

Theorem: Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that

$$n = qa + r$$

and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

Remarks: (1) $q$ is usually called the quotient, and $r$ is called the remainder.

(2) $n$ is divisible by $a$ if and only if $r = 0$. This follows from uniqueness of $q$ and $r$.

(2) The division algorithm is a theorem, not an algorithm. One of the algorithms for finding $q$ and $r$ (for given $n$ and $a$) is called “long division.” It usually assumes that $n \geq 0$.

(3) Existence of $p$ and $q$ is usually proved by using the well-ordering principle.

(4) Note that for $n \geq 0$ the division algorithm is equivalent to writing $n/a$ as a mixed fraction $q + r/a$. 
The division algorithm

Theorem: Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.
The division algorithm

Theorem: Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

Remarks: (1) $q$ is usually called the quotient, and $r$ is called the remainder.
The division algorithm

Theorem: Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

Remarks: (1) $q$ is usually called the quotient, and $r$ is called the remainder. (2) $n$ is divisible by $a$ if and only if $r = 0$. 
The division algorithm

Theorem: Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

Remarks: (1) $q$ is usually called the quotient, and $r$ is called the remainder. (2) $n$ is divisible by $a$ if and only if $r = 0$. This follows from uniqueness of $q$ and $r$. 
The division algorithm

**Theorem:** Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

**Remarks:**
(1) $q$ is usually called the quotient, and $r$ is called the remainder.
(2) $n$ is divisible by $a$ if and only if $r = 0$. This follows from uniqueness of $q$ and $r$.
(3) The division algorithm is a theorem, not an algorithm.
The division algorithm

Theorem: Let \( a \geq 1 \) be an integer. For integer \( n \) there exist two integers, \( q \) and \( r \) such that \( n = qa + r \) and \( 0 \leq r \leq a - 1 \). Moreover the integers \( q \) and \( r \) with these properties are uniquely defined.

Remarks: (1) \( q \) is usually called the quotient, and \( r \) is called the remainder.
(2) \( n \) is divisible by \( a \) if and only if \( r = 0 \). This follows from uniqueness of \( q \) and \( r \).
(2) The division algorithm is a theorem, not an algorithm. One of the algorithms for finding \( q \) and \( r \) (for given \( n \) and \( a \)
The division algorithm

Theorem: Let \( a \geq 1 \) be an integer. For integer \( n \) there exist two integers, \( q \) and \( r \) such that \( n = qa + r \) and \( 0 \leq r \leq a - 1 \). Moreover the integers \( q \) and \( r \) with these properties are uniquely defined.

Remarks: (1) \( q \) is usually called the quotient, and \( r \) is called the remainder.

(2) \( n \) is divisible by \( a \) if and only if \( r = 0 \). This follows from uniqueness of \( q \) and \( r \).

(2) The division algorithm is a theorem, not an algorithm. One of the algorithms for finding \( q \) and \( r \) (for given \( n \) and \( a \)) is called “long division”. It usually assumes that \( n \geq 0 \).
The division algorithm

**Theorem:** Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

**Remarks:**

(1) $q$ is usually called the quotient, and $r$ is called the remainder.

(2) $n$ is divisible by $a$ if and only if $r = 0$. This follows from uniqueness of $q$ and $r$.

(2) The division algorithm is a theorem, not an algorithm. One of the algorithms for finding $q$ and $r$ (for given $n$ and $a$) is called “long division”. It usually assumes that $n \geq 0$.

(3) Existence of $p$ and $q$ is usually proved by using the well-ordering principle.
The division algorithm

**Theorem:** Let $a \geq 1$ be an integer. For integer $n$ there exist two integers, $q$ and $r$ such that $n = qa + r$ and $0 \leq r \leq a - 1$. Moreover the integers $q$ and $r$ with these properties are uniquely defined.

**Remarks:**
1. $q$ is usually called the quotient, and $r$ is called the remainder.
2. $n$ is divisible by $a$ if and only if $r = 0$. This follows from uniqueness of $q$ and $r$.
3. The division algorithm is a theorem, not an algorithm. One of the algorithms for finding $q$ and $r$ (for given $n$ and $a$) is called “long division”. It usually assumes that $n \geq 0$.
4. Existence of $p$ and $q$ is usually proved by using the well-ordering principle.
5. Note that for $n \geq 0$ the division algorithm is equivalent to writing $\frac{n}{a}$ as a mixed fraction $q + \frac{r}{a}$.
Examples of division with remainder

1. $n = 30$ and $a = 7$. What are $q$ and $r$ in this case?

Answer: $q = 4$ and $r = 2$, $30 = 4 \cdot 7 + 2$.

2. $n = 100$ and $a = 20$. What are $q$ and $r$?

Answer: $q = 5$ and $r = 0$, $100 = 5 \cdot 20 + 0$.

3. $n = -17$ and $a = 4$. What are $q$ and $r$?

Answer: $q = -5$ and $r = 3$, $-17 = (-5) \cdot 4 + 3$. 

Math 322, Notes on integers and divisibility  September 13, 2016
Examples of division with remainder

1. $n = 30$ and $a = 7$. What are $q$ and $r$ in this case?
   Answer: $q = 4$ and $r = 2$, $30 = 4 \cdot 7 + 2$. 
Examples of division with remainder

1. $n = 30$ and $a = 7$. What are $q$ and $r$ in this case?
Answer: $q = 4$ and $r = 2$, $30 = 4 \cdot 7 + 2$.

2. $n = 100$ and $a = 20$. What are $q$ and $r$?
Examples of division with remainder

1. \( n = 30 \) and \( a = 7 \). What are \( q \) and \( r \) in this case?
   Answer: \( q = 4 \) and \( r = 2 \), \( 30 = 4 \cdot 7 + 2 \).

2. \( n = 100 \) and \( a = 20 \). What are \( q \) and \( r \)?
   Answer: \( q = 5 \) and \( r = 0 \), \( 100 = 5 \cdot 20 + 0 \).
Examples of division with remainder

1. $n = 30$ and $a = 7$. What are $q$ and $r$ in this case?
Answer: $q = 4$ and $r = 2$, $30 = 4 \cdot 7 + 2$.

2. $n = 100$ and $a = 20$. What are $q$ and $r$?
Answer: $q = 5$ and $r = 0$, $100 = 5 \cdot 20 + 0$.

3. $n = -17$ and $a = 4$. What are $q$ and $r$?
Examples of division with remainder

1. \( n = 30 \) and \( a = 7 \). What are \( q \) and \( r \) in this case?
Answer: \( q = 4 \) and \( r = 2 \), \( 30 = 4 \cdot 7 + 2 \).

2. \( n = 100 \) and \( a = 20 \). What are \( q \) and \( r \)?
Answer: \( q = 5 \) and \( r = 0 \), \( 100 = 5 \cdot 20 + 0 \).

3. \( n = -17 \) and \( a = 4 \). What are \( q \) and \( r \)?
Answer: \( q = -5 \) and \( r = 3 \), \( -17 = (-5) \cdot 4 + 3 \).
Subsets of the integers closed under $+$ and $-$

**Theorem:** Suppose $H$ is a non-empty subset of the integers, closed under $+$ and $-$. Then $H = d\mathbb{Z}$, for some integer $d \geq 0$. That is, $H$ is the set of multiples of $d$.

**Proof:** If 0 is the only element of $H$, then $H = 0\mathbb{Z}$, and we are done. Thus we may assume that $H$ contains some non-zero integer $x$. Then $x - x = 0 \in H$ and $0 - x = -x \in H$. One of the numbers $-x, x$ is positive. Thus $H^+ = \text{set of positive elements of } H$ is non-empty. By the Well Ordering principle, $H^+$ has a minimal element. Denote this minimal element by $d$.

Clearly $d\mathbb{Z} \subset H$. We claim that the converse is true as well, i.e., every $y \in H$ lies in $d\mathbb{Z}$. To prove this, divide $y$ by $d$ with remainder, $y = qd + r$, where $0 \leq r \leq d - 1$. Then $r = y - qd \in H^+$. By minimality of $d$, $r$ cannot be positive, so $r = 0$. Thus $y = dq \in d\mathbb{Z}$, as desired.
Greatest Common Divisor

**Definition:** $a, b$ integers, at least one is non-zero.
**Definition:** $a, b$ integers, at least one is non-zero. 
\[ \text{gcd}(a, b) = \text{greatest common divisor of } a \text{ and } b \]
**Definition:** $a, b$ integers, at least one is non-zero.

$\text{gcd}(a, b) =$ greatest common divisor of $a$ and $b$

is defined as the biggest integer dividing both $a$ and $b$. 
**Definition:** $a, b$ integers, at least one is non-zero. 
\[ \text{gcd}(a, b) = \text{greatest common divisor of } a \text{ and } b \]
is defined as the biggest integer dividing both $a$ and $b$.

An integer linear combination of $a$ and $b$ is an integer of the form

\[ ma + nb, \]

where $n$ and $m$ are integers.
Greatest Common Divisor

**Definition:** $a, b$ integers, at least one is non-zero. $\gcd(a, b) = \text{greatest common divisor of } a \text{ and } b$ is defined as the biggest integer dividing both $a$ and $b$.

An integer linear combination of $a$ and $b$ is an integer of the form

$$ma + nb,$$

where $n$ and $m$ are integers.

Note here we allow $m$ and $n$ to be negative, zero or positive.
A theorem about greatest common divisors

Theorem: \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

Examples 1:
\( a = 7 \), \( b = 5 \).

Q: What is \( \gcd(5, 7) \)?
A: \( \gcd(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?
Q: What are \( m \) and \( n \) here?
A: \( m = 3 \), \( n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \).

Note that this is not the only possible answer. For example, \( m = 10 \), \( n = -7 \) will work as well, \( 1 = 10 \cdot 5 + (-7) \cdot 7 \).

Example 2:
\( a = 9 \), \( b = 15 \).

Q: What is \( \gcd(9, 15) \)?
A: \( \gcd(9, 15) = 3 \).

Q: Can you think of \( m \) and \( n \) such that \( 9m + 15n = 3 \)?
A: \( m = 2 \), \( n = -1 \) will work, \( 3 = 9 \cdot 2 + 15 \cdot (-1) \).

Once again, other answers are possible.
A theorem about greatest common divisors

**Theorem:** $\gcd(a, b)$ equals the smallest positive integer linear combination of $a$ and $b$.

**Examples 1:** $a = 7$, $b = 5$. 

Q: What is $\gcd(5, 7)$?
A: $\gcd(5, 7) = 1$.

Q: What are $m$ and $n$ here?
A: $m = 3$, $n = -2$ works, $1 = 3 \cdot 5 + (-2) \cdot 7$.

Note that this is not the only possible answer. For example, $m = 10$, $n = -7$ will work as well, $1 = 10 \cdot 5 + (-7) \cdot 7$.

**Example 2:** $a = 9$, $b = 15$.

Q: What is $\gcd(9, 15)$?
A: $\gcd(9, 15) = 3$.

Q: Can you think of $m$ and $n$ such that $9m + 15n = 3$?
A: $m = 2$, $n = -1$ will work, $3 = 9 \cdot 2 + 15 \cdot (-1)$.

Once again, other answers are possible.
A theorem about greatest common divisors

**Theorem:** $\text{gcd}(a, b)$ equals the smallest positive integer linear combination of $a$ and $b$.

**Examples 1:** $a = 7$, $b = 5$.
Q: What is $\text{gcd}(5, 7)$?

A: $\text{gcd}(5, 7) = 1$.

The theorem predicts that there exist $m$ and $n$ such that $5m + 7n = 1$?
Q: What are $m$ and $n$ here?
A: $m = 3, n = -2$ works, $1 = 3 \cdot 5 + (-2) \cdot 7$.

Note that this is not the only possible answer. For example, $m = 10, n = -7$ will work as well, $1 = 10 \cdot 5 + (-7) \cdot 7$.

**Example 2:** $a = 9$, $b = 15$.
Q: What is $\text{gcd}(9, 15)$?
A: $\text{gcd}(9, 15) = 3$.
Q: Can you think of $m$ and $n$ such that $9m + 15n = 3$?
A: $m = 2, n = -1$ will work, $3 = 9 \cdot 2 + 15 \cdot (-1)$.

Once again, other answers are possible.
A theorem about greatest common divisors

**Theorem:** \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).

Q: What is \( \gcd(5, 7) \)?  
A: \( \gcd(5, 7) = 1 \).
A theorem about greatest common divisors

**Theorem:** \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).
Q: What is \( \gcd(5, 7) \)? A: \( \gcd(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?

**Notes:**
- For \( a = 7, \ b = 5 \), possible solutions are \( m = 3, \ n = -2 \) and \( m = 10, \ n = -7 \).
- For \( a = 9, \ b = 15 \), possible solutions are \( m = 2, \ n = -1 \) and other solutions are possible.
A theorem about greatest common divisors

**Theorem:** \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).

Q: What is \( \gcd(5, 7) \)?

A: \( \gcd(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?

Q: What are \( m \) and \( n \) here?

A: \( m = 3, \ n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \).

Note that this is not the only possible answer. For example, \( m = 10, \ n = -7 \) will work as well, \( 1 = 10 \cdot 5 + (-7) \cdot 7 \).

Example 2:

\( a = 9, \ b = 15 \).

Q: What is \( \gcd(9, 15) \)?

A: \( \gcd(9, 15) = 3 \).

Q: Can you think of \( m \) and \( n \) such that \( 9m + 15n = 3 \)?

A: \( m = 2, \ n = -1 \) will work, \( 3 = 2 \cdot 9 + (-1) \cdot 15 \).

Once again, other answers are possible.
A theorem about greatest common divisors

**Theorem:** gcd($a$, $b$) equals the smallest positive integer linear combination of $a$ and $b$.

**Examples 1:** $a = 7$, $b = 5$.

Q: What is gcd(5, 7)? A: gcd(5, 7) = 1.

The theorem predicts that there exist $m$ and $n$ such that $5m + 7n = 1$?

Q: What are $m$ and $n$ here?

A: $m = 3$, $n = -2$ works, $1 = 3 \cdot 5 + (-2) \cdot 7$. 

Note that this is not the only possible answer. 
For example, $m = 10$, $n = -7$ will work as well, $1 = 10 \cdot 5 + (-7) \cdot 7$.

Example 2: $a = 9$, $b = 15$.

Q: What is gcd(9, 15)? A: gcd(9, 15) = 3.

Q: Can you think of $m$ and $n$ such that $9m + 15n = 3$?

A: $m = 2$, $n = -1$ will work, $3 = 9 \cdot 2 + 15 \cdot (-1)$.

Once again, other answers are possible.
A theorem about greatest common divisors

**Theorem:** \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).

Q: What is \( \gcd(5, 7) \)? A: \( \gcd(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?

Q: What are \( m \) and \( n \) here?

A: \( m = 3, \ n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \). Note that this is not the only possible answer.
A theorem about greatest common divisors

**Theorem:** \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).

Q: What is \( \gcd(5, 7) \)? A: \( \gcd(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?

Q: What are \( m \) and \( n \) here?

A: \( m = 3, \ n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \). Note that this is not the only possible answer. For example, \( m = 10, \ n = -7 \) will work as well, \( 1 = 10 \cdot 5 + (-7) \cdot 7 \).
Theorem: $\gcd(a, b)$ equals the smallest positive integer linear combination of $a$ and $b$.

Examples 1: $a = 7, \ b = 5$.
Q: What is $\gcd(5, 7)$? A: $\gcd(5, 7) = 1$.

The theorem predicts that there exist $m$ and $n$ such that $5m + 7n = 1$?
Q: What are $m$ and $n$ here?
A: $m = 3, \ n = -2$ works, $1 = 3 \cdot 5 + (-2) \cdot 7$. Note that this is not the only possible answer. For example, $m = 10, \ n = -7$ will work as well, $1 = 10 \cdot 5 + (-7) \cdot 7$.

Example 2: $a = 9, \ b = 15$. 


A theorem about greatest common divisors

**Theorem:** \( \text{gcd}(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).
Q: What is \( \text{gcd}(5, 7) \)?
A: \( \text{gcd}(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?
Q: What are \( m \) and \( n \) here?
A: \( m = 3, \ n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \). Note that this is not the only possible answer. For example, \( m = 10, \ n = -7 \) will work as well, \( 1 = 10 \cdot 5 + (-7) \cdot 7 \).

**Example 2:** \( a = 9, \ b = 15 \).
Q: What is \( \text{gcd}(9, 15) \)?
A theorem about greatest common divisors

**Theorem:** \( \gcd(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).

Q: What is \( \gcd(5, 7) \)? A: \( \gcd(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?

Q: What are \( m \) and \( n \) here?

A: \( m = 3, \ n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \). Note that this is not the only possible answer. For example, \( m = 10, \ n = -7 \) will work as well, \( 1 = 10 \cdot 5 + (-7) \cdot 7 \).

**Example 2:** \( a = 9, \ b = 15 \).

Q: What is \( \gcd(9, 15) \)? A: \( \gcd(9, 15) = 3 \).
A theorem about greatest common divisors

**Theorem:** $\gcd(a, b)$ equals the smallest positive integer linear combination of $a$ and $b$.

**Examples 1:** $a = 7$, $b = 5$.

Q: What is $\gcd(5, 7)$? A: $\gcd(5, 7) = 1$.

The theorem predicts that there exist $m$ and $n$ such that $5m + 7n = 1$?

Q: What are $m$ and $n$ here?

A: $m = 3$, $n = -2$ works, $1 = 3 \cdot 5 + (-2) \cdot 7$. Note that this is not the only possible answer. For example, $m = 10$, $n = -7$ will work as well, $1 = 10 \cdot 5 + (-7) \cdot 7$.

**Example 2:** $a = 9$, $b = 15$.

Q: What is $\gcd(9, 15)$? A: $\gcd(9, 15) = 3$.

Q: Can you think of $m$ and $n$ such that $9m + 15n = 3$?
A theorem about greatest common divisors

**Theorem:** \( \text{gcd}(a, b) \) equals the smallest positive integer linear combination of \( a \) and \( b \).

**Examples 1:** \( a = 7, \ b = 5 \).

Q: What is \( \text{gcd}(5, 7) \)? A: \( \text{gcd}(5, 7) = 1 \).

The theorem predicts that there exist \( m \) and \( n \) such that \( 5m + 7n = 1 \)?

Q: What are \( m \) and \( n \) here?

A: \( m = 3, \ n = -2 \) works, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \). Note that this is not the only possible answer. For example, \( m = 10, \ n = -7 \) will work as well, \( 1 = 10 \cdot 5 + (-7) \cdot 7 \).

**Example 2:** \( a = 9, \ b = 15 \).

Q: What is \( \text{gcd}(9, 15) \)? A: \( \text{gcd}(9, 15) = 3 \).

Q: Can you think of \( m \) and \( n \) such that \( 9m + 15n = 3 \)?

A: \( m = 2, \ n = -1 \) will work, \( 3 = 9 \cdot 2 + 15 \cdot (-1) \).
A theorem about greatest common divisors

**Theorem**: $\gcd(a, b)$ equals the smallest positive integer linear combination of $a$ and $b$.

**Examples 1**: $a = 7$, $b = 5$.

Q: What is $\gcd(5, 7)$? A: $\gcd(5, 7) = 1$.

The theorem predicts that there exist $m$ and $n$ such that $5m + 7n = 1$?

Q: What are $m$ and $n$ here?

A: $m = 3$, $n = -2$ works, $1 = 3 \cdot 5 + (-2) \cdot 7$. Note that this is not the only possible answer. For example, $m = 10$, $n = -7$ will work as well, $1 = 10 \cdot 5 + (-7) \cdot 7$.

**Example 2**: $a = 9$, $b = 15$.

Q: What is $\gcd(9, 15)$? A: $\gcd(9, 15) = 3$.

Q: Can you think of $m$ and $n$ such that $9m + 15n = 3$?

A: $m = 2$, $n = -1$ will work, $3 = 9 \cdot 2 + 15 \cdot (-1)$. Once again, other answers are possible.
Proof of the theorem

Let \( H \) be the set of integer linear combinations of the form \( ma + nb \), where \( m \) and \( n \) range over the integers. Then \( H \) is closed under \(+\) and \(-\) (check!). By the previous theorem, \( H = d\mathbb{Z} \) for some \( d > 1 \).

Here \( d \) is the smallest positive element of \( H \); let us write it as \( d = m_0a + n_0b \).

Since \( a, b \in H \) and \( H = d\mathbb{Z} \), we see that \( d \) divides both \( a \) and \( b \).

On the other hand, if \( e \) is another common divisor of \( a \) and \( b \), then \( e \) divides \( d = m_0a + n_0b \), and hence, \( e \leq d \).

We conclude that \( d \) is the greatest common divisor of \( a \) and \( b \).
Proof of the theorem

Let $H$ be the set of integer linear combinations of the form $ma + nb$, where $m$ and $n$ range over the integers. Then $H$ is closed under $+$ and $-$ (check!). By the previous theorem, $H = d\mathbb{Z}$ for some $d > 1$. 

Since $a, b \in H$ and $H = d\mathbb{Z}$, we see that $d$ divides both $a$ and $b$. On the other hand, if $e$ is another common divisor of $a$ and $b$, then $e$ divides $d = m_0a + n_0b$, and hence, $e \leq d$. We conclude that $d$ is the greatest common divisor of $a$ and $b$. 
Proof of the theorem

Let $H$ be the set of integer linear combinations of the form $ma + nb$, where $m$ and $n$ range over the integers. Then $H$ is closed under $+$ and $-$ (check!). By the previous theorem, $H = d\mathbb{Z}$ for some $d > 1$. Here $d$ is the smallest positive element of $H$; let us write it as $d := m_0a + n_0b$. 
Let $H$ be the set of integer linear combinations of the form $ma + nb$, where $m$ and $n$ range over the integers. Then $H$ is closed under $+$ and $-$ (check!). By the previous theorem, $H = d\mathbb{Z}$ for some $d > 1$. Here $d$ is the smallest positive element of $H$; let us write it as $d := m_0a + n_0b$.

Since $a, b \in H$ and $H = d\mathbb{Z}$, we see that $d$ divides both $a$ and $b$. 
Proof of the theorem

Let $H$ be the set of integer linear combinations of the form $ma + nb$, where $m$ and $n$ range over the integers. Then $H$ is closed under $+$ and $-$ (check!). By the previous theorem, $H = d\mathbb{Z}$ for some $d > 1$. Here $d$ is the smallest positive element of $H$; let us write it as $d := m_0a + n_0b$.

Since $a, b \in H$ and $H = d\mathbb{Z}$, we see that $d$ divides both $a$ and $b$.

On the other hand, if $e$ is another common divisor of $a$ and $b$, then $e$ divides $d = m_0a + n_0b$, and hence, $e \leq d$. 
Proof of the theorem

Let $H$ be the set of integer linear combinations of the form $ma + nb$, where $m$ and $n$ range over the integers. Then $H$ is closed under $+$ and $-$ (check!). By the previous theorem, $H = d\mathbb{Z}$ for some $d > 1$. Here $d$ is the smallest positive element of $H$; let us write it as $d := m_0a + n_0b$.

Since $a, b \in H$ and $H = d\mathbb{Z}$, we see that $d$ divides both $a$ and $b$. On the other hand, if $e$ is another common divisor of $a$ and $b$, then $e$ divides $d = m_0a + n_0b$, and hence, $e \leq d$.

We conclude that $d$ is the greatest common divisor of $a$ and $b$. \qed
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$. 

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof:** If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$. Conversely, suppose $d := \gcd(a, b)$ divides $c$, i.e., $c = dt$ for some integer $t$. By the theorem there exist $m$ and $n$ such that $am + bn = d$. Multiplying both sides of this equality by $t$, we see that $a(mt) + b(nt) = dt = c$. Thus $x := mt$ and $y := nt$ satisfy $ax + by = c$, as desired.
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$. 

Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$. 

---

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof:** If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$.

Conversely, suppose $d := \gcd(a, b)$ divides $c$, i.e., $c = dt$ for some integer $t$.

By the theorem there exist $m$ and $n$ such that $am + bn = d$.

Multiplying both sides of this equality by $t$, we see that $a(mt) + b(nt) = dt = c$.

Thus $x := mt$ and $y := nt$ satisfy $ax + by = c$, as desired.
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$.

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$.

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides \( \gcd(a, b) \).

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$. Conversely, if $e$ divides both $a$ and $b$, then $e$ divides \( \gcd(a, b) = ma + nb \).

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof:** If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$. 
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$.

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof:** If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$.

Conversely, suppose $d := \gcd(a, b)$ divides $c$, i.e., $c = dt$ for some integer $t$. 
Two corollaries

**Corollary 1:** An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof:** By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$.

**Corollary 2:** Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof:** If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$.

Conversely, suppose $d := \gcd(a, b)$ divides $c$, i.e., $c = dt$ for some integer $t$. By the theorem there exist $m$ and $n$ such that $am + bn = d$. 
Two corollaries

Corollary 1: An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

Proof: By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$.

Corollary 2: Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

Proof: If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$.

Conversely, suppose $d := \gcd(a, b)$ divides $c$, i.e., $c = dt$ for some integer $t$. By the theorem there exist $m$ and $n$ such that $am + bn = d$. Multiplying both sides of this equality by $t$, we see that $a(mt) + b(nt) = dt = c$. 

Math 322, Notes on integers and divisibility
Two corollaries

**Corollary 1**: An integer $e$ is a common divisor of $a$ and $b$ if and only if $e$ divides $\gcd(a, b)$.

**Proof**: By definition, $d$ divides both $a$ and $b$. Thus if $e$ divides $d$, then $e$ divides both $a$ and $b$.

Conversely, if $e$ divides both $a$ and $b$, then $e$ divides $\gcd(a, b) = ma + nb$.

**Corollary 2**: Let $c$ be an integer. Then the equation $ax + by = c$ has an integer solution if and only if $c$ is divisible by $\gcd(a, b)$.

**Proof**: If $ax + by = c$ for some integers $x$ and $y$, then clearly $\gcd(a, b)$ divides $c$.

Conversely, suppose $d := \gcd(a, b)$ divides $c$, i.e., $c = dt$ for some integer $t$. By the theorem there exist $m$ and $n$ such that $am + bn = d$. Multiplying both sides of this equality by $t$, we see that $a(mt) + b(nt) = dt = c$. Thus $x := mt$ and $y := nt$ satisfy $ax + by = c$, as desired.
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$. 
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$. 

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all "prime" (i.e., none of them can be written as a product of two even integers), and $300 = 10 \cdot 30 = 6 \cdot 50$ can be written as a product of "primes" in two different ways. The point is: the fundamental theorem of arithmetic is not obvious, it requires proof.
The fundamental theorem of arithmetic

Every positive integer \( n > 1 \) can be written as a product of (not necessarily distinct) primes, \( n = p_1 \ldots p_r \). Moreover, up to reordering, the prime factors \( p_1, \ldots, p_r \) are uniquely determined by \( n \).

Examples: \( 60 = 2 \cdot 2 \cdot 3 \cdot 5 \).
\( 724 = 2 \cdot 2 \cdot 181 \).
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.
$724 = 2 \cdot 2 \cdot 181$.
$100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73$. 

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime” (i.e., none of them can be written as a product of two even integers), and $300 = 10 \cdot 30 = 6 \cdot 50$ can be written as a product of “primes” in two different ways. The point is: the fundamental theorem of arithmetic is not obvious, it requires proof.
Every positive integer \( n > 1 \) can be written as a product of (not necessarily distinct) primes, \( n = p_1 \ldots p_r \). Moreover, up to reordering, the prime factors \( p_1, \ldots, p_r \) are uniquely determined by \( n \).

Examples: \( 60 = 2 \cdot 2 \cdot 3 \cdot 5 \).
\( 724 = 2 \cdot 2 \cdot 181 \).
\( 100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73 \).

Remark: The fundamental theorem of arithmetic is not true
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.
$724 = 2 \cdot 2 \cdot 181$.
$100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73$.

Remark: The fundamental theorem of arithmetic is not true in some other number systems.
Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.
$724 = 2 \cdot 2 \cdot 181$.
$100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73$.

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime”
The fundamental theorem of arithmetic

Every positive integer \( n > 1 \) can be written as a product of (not necessarily distinct) primes, \( n = p_1 \ldots p_r \). Moreover, up to reordering, the prime factors \( p_1, \ldots, p_r \) are uniquely determined by \( n \).

Examples: \( 60 = 2 \cdot 2 \cdot 3 \cdot 5 \).
\( 724 = 2 \cdot 2 \cdot 181 \).
\( 100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73 \).

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime” (i.e., none of them can be written as a product of two even integers),
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.  
$724 = 2 \cdot 2 \cdot 181$.  
$100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73$.  

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime” (i.e., none of them can be written as a product of two even integers), and

$$300 = 10 \cdot 30 = 6 \cdot 50$$
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.
$724 = 2 \cdot 2 \cdot 181$.
$100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73$.

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime” (i.e., none of them can be written as a product of two even integers), and

$$300 = 10 \cdot 30 = 6 \cdot 50$$

can be written as a product of “primes” in two different ways.
The fundamental theorem of arithmetic

Every positive integer \( n > 1 \) can be written as a product of (not necessarily distinct) primes, \( n = p_1 \ldots p_r \). Moreover, up to reordering, the prime factors \( p_1, \ldots, p_r \) are uniquely determined by \( n \).

Examples: \( 60 = 2 \cdot 2 \cdot 3 \cdot 5 \).
\( 724 = 2 \cdot 2 \cdot 181 \).
\( 100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73 \).

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime” (i.e., none of them can be written as a product of two even integers), and

\[ 300 = 10 \cdot 30 = 6 \cdot 50 \]

can be written as a product of “primes” in two different ways. The point is: the fundamental theorem of arithmetic is not obvious,
The fundamental theorem of arithmetic

Every positive integer $n > 1$ can be written as a product of (not necessarily distinct) primes, $n = p_1 \ldots p_r$. Moreover, up to reordering, the prime factors $p_1, \ldots, p_r$ are uniquely determined by $n$.

Examples: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.
$724 = 2 \cdot 2 \cdot 181$.
$100375 = 5 \cdot 5 \cdot 5 \cdot 11 \cdot 73$.

Remark: The fundamental theorem of arithmetic is not true in some other number systems. For example, if we only consider even numbers, then 6, 10, 30, 50 are all “prime” (i.e., none of them can be written as a product of two even integers), and

$$300 = 10 \cdot 30 = 6 \cdot 50$$

can be written as a product of “primes” in two different ways. The point is: the fundamental theorem of arithmetic is not obvious, it requires proof.
We have previously proved the existence of a prime decomposition

\[ n = p_1 \ldots p_r. \]
We have previously proved the existence of a prime decomposition $n = p_1 \ldots p_r$. To prove uniqueness, we will need the following
Proof of the Fundamental Theorem of Arithmetic I

We have previously proved the existence of a prime decomposition $n = p_1 \ldots p_r$. To prove uniqueness, we will need the following Lemma: If $a$ divides $bc$, and $\gcd(a, b) = 1$, then $a$ divides $c$. 

**Lemma:** If $a$ divides $bc$, and $\gcd(a, b) = 1$, then $a$ divides $c$. 

Remark: Note that the lemma fails, if we do not assume that $\gcd(a, b) = 1$. For example, take $a = 6$, $b = 3$ and $c = 4$. Then 6 divides $3 \cdot 4 = 12$, but 6 does not divide 4.
Proof of the Fundamental Theorem of Arithmetic I

We have previously proved the existence of a prime decomposition $n = p_1 \cdots p_r$. To prove uniqueness, we will need the following

Lemma: If $a$ divides $bc$, and $\gcd(a, b) = 1$, then $a$ divides $c$.

Proof: Since $\gcd(a, b) = 1$, ...
We have previously proved the existence of a prime decomposition \( n = p_1 \ldots p_r \). To prove uniqueness, we will need the following

**Lemma:** If \( a \) divides \( bc \), and \( \gcd(a, b) = 1 \), then \( a \) divides \( c \).

**Proof:** Since \( \gcd(a, b) = 1 \), there exist integers \( x \) and \( y \)
We have previously proved the existence of a prime decomposition \( n = p_1 \ldots p_r \). To prove uniqueness, we will need the following Lemma:

**Lemma:** If \( a \) divides \( bc \), and \( \gcd(a, b) = 1 \), then \( a \) divides \( c \).

**Proof:** Since \( \gcd(a, b) = 1 \), there exist integers \( x \) and \( y \) such that

\[
ax + by = 1.
\]

Now multiply this equality by \( c \):
We have previously proved the existence of a prime decomposition \( n = p_1 \ldots p_r \). To prove uniqueness, we will need the following

**Lemma:** If \( a \) divides \( bc \), and \( \gcd(a, b) = 1 \), then \( a \) divides \( c \).

**Proof:** Since \( \gcd(a, b) = 1 \), there exist integers \( x \) and \( y \) such that \( ax + by = 1 \). Now multiply this equality by \( c \):

\[
acx + bc y = c .
\]

Both terms on the left hand side are divisible by \( a \). Hence, \( c \) is also divisible by \( a \). \( \square \)
We have previously proved the existence of a prime decomposition
\( n = p_1 \ldots p_r \). To prove uniqueness, we will need the following

**Lemma:** If \( a \) divides \( bc \), and \( \gcd(a, b) = 1 \), then \( a \) divides \( c \).

**Proof:** Since \( \gcd(a, b) = 1 \), there exist integers \( x \) and \( y \) such that
\[
ax + by = 1.
\]
Now multiply this equality by \( c \):
\[
acx + bcy = c.
\]
Both terms on the left hand side are divisible by \( a \). Hence, \( c \) is also divisible by \( a \).

**Remark:** Note that the lemma fails, if we do not assume that \( \gcd(a, b) = 1 \). For example, take \( a = 6, b = 3 \) and \( c = 4 \). Then 6 divides \( 3 \cdot 4 = 12 \), but 6 does not divide 4.
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. 
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$. 
**Corollary:** Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

**Proof:** Argue by induction on $r$, 

Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

Proof: Argue by induction on $r$, starting from $r = 1$. 

\[\square\]
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

Proof: Argue by induction on $r$, starting from $r = 1$.

Proof of the Fundamental Theorem of Arithmetic:
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

Proof: Argue by induction on $r$, starting from $r = 1$.

Proof of the Fundamental Theorem of Arithmetic: Assume that some integer $n$ can be written as a product of primes
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

Proof: Argue by induction on $r$, starting from $r = 1$.

Proof of the Fundamental Theorem of Arithmetic: Assume that some integer $n$ can be written as a product of primes in two different ways,

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

Proof: Argue by induction on $r$, starting from $r = 1$. \hfill \Box

Proof of the Fundamental Theorem of Arithmetic: Assume that some integer $n$ can be written as a product of primes in two different ways,

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

where $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes. After cancelling all primes that occur on both sides,
Corollary: Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

Proof: Argue by induction on $r$, starting from $r = 1$.

Proof of the Fundamental Theorem of Arithmetic: Assume that some integer $n$ can be written as a product of primes in two different ways,

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

where $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes. After cancelling all primes that occur on both sides, we may assume $p_i \neq q_j$. 
Conclusion of the proof

**Corollary:** Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

**Proof:** Argue by induction on $r$, starting from $r = 1$.

**Proof of the Fundamental Theorem of Arithmetic:** Assume that some integer $n$ can be written as a product of primes in two different ways,

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

where $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes. After cancelling all primes that occur on both sides, we may assume $p_i \neq q_j$ for any $i = 1, \ldots, r$ and any $j = 1, \ldots, s$. 


Conclusion of the proof

**Corollary:** Suppose a prime $p$ divides the product $a_1 \cdot a_2 \ldots a_r$. Then $p$ divides (at least) one of the integers $a_1, \ldots, a_r$.

**Proof:** Argue by induction on $r$, starting from $r = 1$.

**Proof of the Fundamental Theorem of Arithmetic:** Assume that some integer $n$ can be written as a product of primes in two different ways,

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

where $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes. After cancelling all primes that occur on both sides, we may assume $p_i \neq q_j$ for any $i = 1, \ldots, r$ and any $j = 1, \ldots, s$. By the corollary, $p_1$ divides one of the primes $q_1, \ldots, q_s$, a contradiction.
The least common multiple of $a$ and $b$

\[
lcm(a, b) \text{ is the smallest positive integer},
\]
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. 

Example: $gcd(50771, 4326) = 7$. Hence, $lcm(50771, 4326) = \frac{50771 \cdot 4326}{gcd(50771, 4326)} = \frac{50771 \cdot 4326}{7} = 31,376,478$. 

Math 322, Notes on integers and divisibility  
September 13, 2016
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$. 

The least common multiple of \( a \) and \( b \)

\( \text{lcm}(a, b) \) is the smallest positive integer, which is a divisible by both \( a \) and \( b \). Here \( a, b \neq 0 \).

**Proposition:** Suppose \( a = p_1^{d_1} \ldots p_r^{d_r} \)
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \ldots p_r^{d_r}$ and $b = p_1^{e_1} \ldots p_r^{e_r}$,
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \ldots p_r^{d_r}$ and $b = p_1^{e_1} \ldots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and
The least common multiple of $a$ and $b$

lcm$(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \ldots p_r^{d_r}$ and $b = p_1^{e_1} \ldots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \cdots p_r^{d_r}$ and $b = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then

(a) $gcd(a, b) = p_1^{\min(d_1,e_1)} \cdots p_r^{\min(d_r,e_r)}$. 

(b) $lcm(a, b) = p_1^{\max(d_1,e_1)} \cdots p_r^{\max(d_r,e_r)}$. 

(c) $gcd(a, b) \cdot lcm(a, b) = ab$. 

Example: $gcd(50771, 4326) = 7$. 

Hence, $lcm(50771, 4326) = 50771 \cdot 4326 \cdot \frac{1}{gcd(50771, 4326)} = \frac{31 \cdot 376 \cdot 478}{7}$. 

Math 322, Notes on integers and divisibility

September 13, 2016
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \cdots p_r^{d_r}$ and $b = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then

(a) $gcd(a, b) = p_1^{\min(d_1,e_1)} \cdots p_r^{\min(d_r,e_r)}$.

(b) $lcm(a, b) = p_1^{\max(d_1,e_1)} \cdots p_r^{\max(d_r,e_r)}$.
The least common multiple of \( a \) and \( b \)

\( \text{lcm}(a, b) \) is the smallest positive integer, which is a divisible by both \( a \) and \( b \). Here \( a, b \neq 0 \).

**Proposition:** Suppose \( a = p_1^{d_1} \ldots p_r^{d_r} \) and \( b = p_1^{e_1} \ldots p_r^{e_r} \), where \( p_1, \ldots, p_r \) are distinct primes, and \( d_1, \ldots, d_r, e_1, \ldots, e_r \) are non-negative integers. Then

(a) \( \gcd(a, b) = p_1^{\min(d_1, e_1)} \ldots p_r^{\min(d_r, e_r)} \).

(b) \( \text{lcm}(a, b) = p_1^{\max(d_1, e_1)} \ldots p_r^{\max(d_r, e_r)} \).

(c) \( \gcd(a, b) \text{lcm}(a, b) = ab \).

Example: \( \gcd(50771, 4326) = 7 \). Hence, \( \text{lcm}(50771, 4326) = \frac{50771 \cdot 4326}{7} = 31,376,378 \).
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \ldots p_r^{d_r}$ and $b = p_1^{e_1} \ldots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then

(a) $gcd(a, b) = p_1^{\min(d_1, e_1)} \ldots p_r^{\min(d_r, e_r)}$.

(b) $lcm(a, b) = p_1^{\max(d_1, e_1)} \ldots p_r^{\max(d_r, e_r)}$.

(c) $gcd(a, b) \cdot lcm(a, b) = ab$.

Example: $gcd(50771, 4326) = 7$. 
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \cdots p_r^{d_r}$ and $b = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then

(a) $gcd(a, b) = p_1^{\min(d_1,e_1)} \cdots p_r^{\min(d_r,e_r)}$.
(b) $lcm(a, b) = p_1^{\max(d_1,e_1)} \cdots p_r^{\max(d_r,e_r)}$.
(c) $gcd(a, b)lcm(a, b) = ab$.

Example: $gcd(50771, 4326) = 7$. Hence,

$$lcm(50771, 4326) = \cdots$$
The least common multiple of \(a\) and \(b\)

\[\text{lcm}(a, b)\] is the smallest positive integer, which is a divisible by both \(a\) and \(b\). Here \(a, b \neq 0\).

**Proposition:** Suppose \(a = p_1^{d_1} \ldots p_r^{d_r}\) and \(b = p_1^{e_1} \ldots p_r^{e_r}\), where \(p_1, \ldots, p_r\) are distinct primes, and \(d_1, \ldots, d_r, e_1, \ldots, e_r\) are non-negative integers. Then

(a) \(\gcd(a, b) = p_1^{\min(d_1, e_1)} \ldots p_r^{\min(d_r, e_r)}\).

(b) \(\text{lcm}(a, b) = p_1^{\max(d_1, e_1)} \ldots p_r^{\max(d_r, e_r)}\).

(c) \(\gcd(a, b) \cdot \text{lcm}(a, b) = ab\).

Example: \(\gcd(50771, 4326) = 7\). Hence,

\[
\text{lcm}(50771, 4326) = \frac{50771 \cdot 4326}{\gcd(50771, 4326)} =
\]
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \ldots p_r^{d_r}$ and $b = p_1^{e_1} \ldots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then

(a) $gcd(a, b) = p_1^{\min(d_1, e_1)} \ldots p_r^{\min(d_r, e_r)}$.

(b) $lcm(a, b) = p_1^{\max(d_1, e_1)} \ldots p_r^{\max(d_r, e_r)}$.

(c) $gcd(a, b)lcm(a, b) = ab$.

Example: $gcd(50771, 4326) = 7$. Hence,

$$lcm(50771, 4326) = \frac{50771 \cdot 4326}{gcd(50771, 4326)} = \frac{50771 \cdot 4326}{7} =$$
The least common multiple of $a$ and $b$

$lcm(a, b)$ is the smallest positive integer, which is a divisible by both $a$ and $b$. Here $a, b \neq 0$.

**Proposition:** Suppose $a = p_1^{d_1} \cdots p_r^{d_r}$ and $b = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes, and $d_1, \ldots, d_r, e_1, \ldots, e_r$ are non-negative integers. Then

(a) $gcd(a, b) = p_1^{\min(d_1,e_1)} \cdots p_r^{\min(d_r,e_r)}$.

(b) $lcm(a, b) = p_1^{\max(d_1,e_1)} \cdots p_r^{\max(d_r,e_r)}$.

(c) $gcd(a, b) \cdot lcm(a, b) = ab$.

Example: $gcd(50771, 4326) = 7$. Hence,

$$lcm(50771, 4326) = \frac{50771 \cdot 4326}{gcd(50771, 4326)} = \frac{50771 \cdot 4326}{7} = 31,376,478.$$