Definition: $a, b$ integers, at least one is non-zero.
Greatest Common Divisor

**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.

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

is defined as the biggest integer dividing both $a$ and $b$. 
Greatest Common Divisor

**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 $b$.

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. \( \gcd(a, b) = \) greatest common divisor of \( a \) 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, \( 3 = 2 \cdot 9 + (-1) \cdot 15 \).
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: \( \gcd(5, 7) = 1 \).

Q: Can you think of \( m \) and \( n \) such that \( 5m + 7n = 1 \)?
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.

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: \( \gcd(5, 7) = 1 \).
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 \( 5m + 7n = 1 \)?
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 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, \( 1 = 3 \cdot 5 + (-2) \cdot 7 \).
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, \(1 = 10 \cdot 5 + (-7) \cdot 7\).
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:** $a = 9$, $b = 15$. 

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 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:** \( \gcd(a, b) \) 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, \( 3 = 9 \cdot 2 + 15 \cdot (-1) \).
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

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that (i) $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and (ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$.

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$.

Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$. (Check!) This contradicts the minimality of $d$.

To prove (ii), note that every integer $e$ dividing both $a$ and $b$ will also divide $d = m_0a + n_0b$. Thus $e \leq d$. 

Math 312, Lecture 4

September 16, 2015
By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. 
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$. 

Math 312, Lecture 4
September 16, 2015
By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$. We want to show that $d = \gcd(a, b)$. 

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$. (Check!) This contradicts the minimality of $d$.

To prove (ii), note that every integer $e$ dividing both $a$ and $b$ will also divide $d = m_0a + n_0b$. Thus $e \leq d$. 

Math 312, Lecture 4  
September 16, 2015
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that
(i) $d$ is a common divisor of $a$ and $b$,
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that (i) $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form \( ma + nb \). Let us denote it by \( d := m_0 a + n_0 b \).

We want to show that \( d = \gcd(a, b) \). That is, we want to show that

(i) \( d \) is a common divisor of \( a \) and \( b \), i.e., \( d \) divides both \( a \) and \( b \), and

(ii) \( d \) is the greatest common divisor,
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that
(i) $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and
(ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$. 

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r ≤ d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$. (Check!) This contradicts the minimality of $d$.

To prove (ii), note that every integer $e$ dividing both $a$ and $b$ will also divide $d = m_0a + n_0b$. Thus $e ≤ d$. 

Math 312, Lecture 4

September 16, 2015
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that

(i) $d$ is a commond divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and
(ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$.

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. 

Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$. (Check!) This contradicts the minimality of $d$.

To prove (ii), note that every integer $e$ dividing both $a$ and $b$ will also divide $d = m_0a + n_0b$. Thus $e \leq d$. 

Math 312, Lecture 4
September 16, 2015
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that

(i) $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and

(ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$.

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, 

\[ r = a - (m_0a + n_0b) = (1 - m_0)a - n_0b. \]

This contradicts the minimality of $d$.

To prove (ii), note that every integer $e$ dividing both $a$ and $b$ will also divide $d = m_0a + n_0b$. Thus $e \leq d$.
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that
(i) $d$ is a commond divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and
(ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$.

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$.
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that (i) $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and (ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$.

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$. (Check!)
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form $ma + nb$. Let us denote it by $d := m_0a + n_0b$.

We want to show that $d = \gcd(a, b)$. That is, we want to show that (i) $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$, and (ii) $d$ is the greatest common divisor, i.e., if $e$ is another common divisor of $a$ and $b$, then $e < d$.

To prove (i), we argue by contradiction. Assume the contrary, say, $d$ does not divide $a$. Divide $a$ by $d$ with remainder, $a = qd + r$, where $0 < r \leq d - 1$. Substituting $d = m_0a + n_0b$ into $r = a - qd$, we see that $r$ is an integer linear combination of $a$ and $b$. (Check!) This contradicts the minimality of $d$. 
Proof of the theorem

By the well-ordering principle there exists the smallest positive integer of the form \( ma + nb \). Let us denote it by \( d := m_0a + n_0b \).

We want to show that \( d = \gcd(a, b) \). That is, we want to show that

(i) \( d \) is a common divisor of \( a \) and \( b \), i.e., \( d \) divides both \( a \) and \( b \), and
(ii) \( d \) is the greatest common divisor,
i.e., if \( e \) is another common divisor of \( a \) and \( b \), then \( e < d \).

To prove (i), we argue by contradiction. Assume the contrary, say, \( d \) does not divide \( a \). Divide \( a \) by \( d \) with remainder, \( a = qd + r \), where \( 0 < r \leq d - 1 \). Substituting \( d = m_0a + n_0b \) into \( r = a - qd \), we see that \( r \) is an integer linear combination of \( a \) and \( b \). (Check!) This contradicts the minimality of \( d \).

To prove (ii), note that every integer \( e \) dividing both \( a \) and \( b \) will also divide \( d = m_0a + n_0b \). Thus \( e \leq d \).
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 $a(mt) + b(nt) = dt = c$.

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 $b$. 
**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 $\text{gcd}(a, b)$.

**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 $\text{gcd}(a, b) = ma + nb$. 

**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 $\text{gcd}(a, b)$. 

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 $c$. 

Math 312, Lecture 4

September 16, 2015
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 $a(mt) + b(nt) = dt = c$. 

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.
Computing $\gcd(a, b)$ for large integers $a$ and $b$ is an important practical problem.
Computing $\text{gcd}(a, b)$ for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type.
The Euclidean algorithm

Computing gcd($a, b$) for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive.
The Euclidean algorithm

Computing $\gcd(a, b)$ for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing $\gcd(a, b)$.
The Euclidean algorithm

Computing gcd(a, b) for large integers a and b is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing gcd(a, b). It only tells us that gcd(a, b) is the minimal positive number of the form ax + by.
The Euclidean algorithm

Computing \( \gcd(a, b) \) for large integers \( a \) and \( b \) is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing \( \gcd(a, b) \). It only tells us that \( \gcd(a, b) \) is the minimal positive number of the form \( ax + by \). Here \( x \) and \( y \) range over infinitely many possible integer values,
The Euclidean algorithm

Computing gcd\((a, b)\) for large integers \(a\) and \(b\) is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing gcd\((a, b)\). It only tells us that gcd\((a, b)\) is the minimal positive number of the form \(ax + by\). Here \(x\) and \(y\) range over infinitely many possible integer values, and we cannot check them all.
The Euclidean algorithm

Computing \( \gcd(a, b) \) for large integers \( a \) and \( b \) is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing \( \gcd(a, b) \). It only tells us that \( \gcd(a, b) \) is the minimal positive number of the form \( ax + by \). Here \( x \) and \( y \) range over infinitely many possible integer values, and we cannot check them all. Factoring \( a \) and \( b \) in order to find \( \gcd(a, b) \) works for small \( a \) and \( b \),
The Euclidean algorithm

Computing gcd($a$, $b$) for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing gcd($a$, $b$). It only tells us that gcd($a$, $b$) is the minimal positive number of the form $ax + by$. Here $x$ and $y$ range over infinitely many possible integer values, and we cannot check them all. Factoring $a$ and $b$ in order to find gcd($a$, $b$) works for small $a$ and $b$, but becomes impractical when $a$ and $b$ are large (say, several hundred digits).
Computing $\gcd(a, b)$ for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing $\gcd(a, b)$. It only tells us that $\gcd(a, b)$ is the minimal positive number of the form $ax + by$. Here $x$ and $y$ range over infinitely many possible integer values, and we cannot check them all. Factoring $a$ and $b$ in order to find $\gcd(a, b)$ works for small $a$ and $b$, but becomes impractical when $a$ and $b$ are large (say, several hundred digits). Fortunately, there is a highly recursive (and thus easily programmable)
The Euclidean algorithm

Computing $\gcd(a, b)$ for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing $\gcd(a, b)$. It only tells us that $\gcd(a, b)$ is the minimal positive number of the form $ax + by$. Here $x$ and $y$ range over infinitely many possible integer values, and we cannot check them all.

Factoring $a$ and $b$ in order to find $\gcd(a, b)$ works for small $a$ and $b$, but becomes impractical when $a$ and $b$ are large (say, several hundred digits). Fortunately, there is a highly recursive (and thus easily programmable) fast algorithm for computing $\gcd(a, b)$, called the Euclidean algorithm.
The Euclidean algorithm

Computing \( \gcd(a, b) \) for large integers \( a \) and \( b \) is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing \( \gcd(a, b) \). It only tells us that \( \gcd(a, b) \) is the minimal positive number of the form \( ax + by \). Here \( x \) and \( y \) range over infinitely many possible integer values, and we cannot check them all.

Factoring \( a \) and \( b \) in order to find \( \gcd(a, b) \) works for small \( a \) and \( b \), but becomes impractical when \( a \) and \( b \) are large (say, several hundred digits). Fortunately, there is a highly recursive (and thus easily programmable) fast algorithm for computing \( \gcd(a, b) \), called the \textit{Euclidean algorithm}.

Here “fast” means that the amount of time required to run it is...
The Euclidean algorithm

Computing $\gcd(a, b)$ for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing $\gcd(a, b)$. It only tells us that $\gcd(a, b)$ is the minimal positive number of the form $ax + by$. Here $x$ and $y$ range over infinitely many possible integer values, and we cannot check them all.

Factoring $a$ and $b$ in order to find $\gcd(a, b)$ works for small $a$ and $b$, but becomes impractical when $a$ and $b$ are large (say, several hundred digits).

Fortunately, there is a highly recursive (and thus easily programmable) fast algorithm for computing $\gcd(a, b)$, called the *Euclidean algorithm*. Here “fast” means that the amount of time required to run it is at most a constant multiple of $\log_2(\max(a, b))$. 
The Euclidean algorithm

Computing gcd($a, b$) for large integers $a$ and $b$ is an important practical problem. Most cryptographic algorithms rely on computations of this type. The theorem we just proved is non-constructive. That is, it does not give us a practical way of computing gcd($a, b$). It only tells us that gcd($a, b$) is the minimal positive number of the form $ax + by$. Here $x$ and $y$ range over infinitely many possible integer values, and we cannot check them all. Factoring $a$ and $b$ in order to find gcd($a, b$) works for small $a$ and $b$, but becomes impractical when $a$ and $b$ are large (say, several hundred digits). Fortunately, there is a highly recursive (and thus easily programmable) fast algorithm for computing gcd($a, b$), called the Euclidean algorithm. Here “fast” means that the amount of time required to run it is at most a constant multiple of $\log_2(\max(a, b))$. In short the Euclidean algorithm runs in “logarithmic time”.
To explain how the Euclidean algorithm works,
To explain how the Euclidean algorithm works, I need the following:

Lemma:

\[ \gcd(a, b) = \gcd(a + nb, b) \]

for any integer \( n \).

Proof:
The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

Corollary:

Let \( r \) be the remainder of division of \( a \) by \( b \).

That is, \( a = bq + r \).

Then \( \gcd(a, b) = \gcd(b, r) \).

Proof:

Note that \( r = a - bq \).

Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively.

We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \).

Each subsequent step consists of replacing \((a, b)\) by \((b, r)\).

This does not change the gcd, and both \( a \) and \( b \) become smaller.

Continue as long as the second number remains positive.

We stop when \( r = 0 \).

At this point \( \gcd(b, r) = \gcd(b, 0) = b \), and we are done.
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

Corollary: Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - bq \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively. We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \). Each subsequent step consists of replacing \( (a, b) \) by \( (b, r) \). This does not change the gcd, and both \( a \) and \( b \) become smaller. Continue as long as the second number remains positive. We stop when \( r = 0 \). At this point \( \gcd(b, r) = \gcd(b, 0) = b \), and we are done.
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** $\gcd(a, b) = \gcd(a + nb, b)$ for any integer $n$.

**Proof:** The common divisors of $a$ and $b$ are the same as the common divisors of $a + nb$ and $b$. (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let $r$ be the remainder of division of $a$ by $b$. 
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma**: $\gcd(a, b) = \gcd(a + nb, b)$ for any integer $n$.

**Proof**: The common divisors of $a$ and $b$ are the same as the common divisors of $a + nb$ and $b$. (Check!) Thus the greatest common divisor is the same.

**Corollary**: Let $r$ be the remainder of division of $a$ by $b$. That is, $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$. 
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \).
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** $\gcd(a, b) = \gcd(a + nb, b)$ for any integer $n$.

**Proof:** The common divisors of $a$ and $b$ are the same as the common divisors of $a + nb$ and $b$. (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let $r$ be the remainder of division of $a$ by $b$. That is, $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

**Proof:** Note that $r = a - qb$. Now apply the lemma with $n = -q$. 

A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively.
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively. We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \).
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively. We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \). Each subsequent step consists of replacing \( (a, b) \) by \( (b, r) \).
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively. We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \). Each subsequent step consists of replacing \((a, b)\) by \((b, r)\). This does not change the gcd,
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** $\gcd(a, b) = \gcd(a + nb, b)$ for any integer $n$.

**Proof:** The common divisors of $a$ and $b$ are the same as the common divisors of $a + nb$ and $b$. (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let $r$ be the remainder of division of $a$ by $b$. That is, $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

**Proof:** Note that $r = a - qb$. Now apply the lemma with $n = -q$.

The Euclidean algorithm applies the above corollary recursively. We arrange $a, b$ so that $a \geq b$ and $b > 0$. Each subsequent step consists of replacing $(a, b)$ by $(b, r)$. This does not change the gcd, and both $a$ and $b$ become smaller.
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively. We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \). Each subsequent step consists of replacing \((a, b)\) by \((b, r)\). This does not change the gcd, and both \( a \) and \( b \) become smaller. Continue as long as the second number remains positive.
To explain how the Euclidean algorithm works, I need the following:

**Lemma:** \( \gcd(a, b) = \gcd(a + nb, b) \) for any integer \( n \).

**Proof:** The common divisors of \( a \) and \( b \) are the same as the common divisors of \( a + nb \) and \( b \). (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let \( r \) be the remainder of division of \( a \) by \( b \). That is, \( a = bq + r \). Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:** Note that \( r = a - qb \). Now apply the lemma with \( n = -q \).

The Euclidean algorithm applies the above corollary recursively. We arrange \( a, b \) so that \( a \geq b \) and \( b > 0 \). Each subsequent step consists of replacing \((a, b)\) by \((b, r)\). This does not change the gcd, and both \( a \) and \( b \) become smaller. Continue as long as the second number remains positive. We stop when \( r = 0 \).
A lemma

To explain how the Euclidean algorithm works, I need the following:

**Lemma:** $\gcd(a, b) = \gcd(a + nb, b)$ for any integer $n$.

**Proof:** The common divisors of $a$ and $b$ are the same as the common divisors of $a + nb$ and $b$. (Check!) Thus the greatest common divisor is the same.

**Corollary:** Let $r$ be the remainder of division of $a$ by $b$. That is, $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

**Proof:** Note that $r = a - qb$. Now apply the lemma with $n = -q$.

The Euclidean algorithm applies the above corollary recursively. We arrange $a, b$ so that $a \geq b$ and $b > 0$. Each subsequent step consists of replacing $(a, b)$ by $(b, r)$. This does not change the gcd, and both $a$ and $b$ become smaller. Continue as long as the second number remains positive. We stop when $r = 0$. At this point $\gcd(b, r) = \gcd(b, 0) = b$, and we are done.
Example 1: $a = 30, \ b = 18$. 

Step 1: Divide $30$ by $18$. 

$$30 = 1 \cdot 18 + 12.$$ 
Replace $(30, 18)$ by $(18, 12)$.  

Step 2: Divide $18$ by $12$. 

$$18 = 1 \cdot 12 + 6.$$ 
Replace $(18, 12)$ by $(12, 6)$. 

Step 3: Divide $12$ by $6$. 

$$12 = 2 \cdot 6 + 0.$$ 
Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$. 

In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$. 

Example 2: $a = 3600, \ b = 1065$. 

Once again, we divide $3600$ by $1065$ with remainder: 

$$3600 = 3 \cdot 1065 + 405,$$ 
replace $(3600, 1065)$ by $(1065, 405)$, 
and proceed recursively. 

$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15$. 

Math 312, Lecture 4, September 16, 2015
The Euclidean algorithm in action

Example 1: $a = 30, b = 18$.

Step 1: Divide 30 by 18.

$$30 = 1 \cdot 18 + 12.$$

Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12.

$$18 = 1 \cdot 12 + 6.$$

Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6.

$$12 = 2 \cdot 6 + 0.$$

Replace $(12, 6)$ by $(6, 0)$.

Now $\text{gcd}(6, 0) = 6$.

In summary, $\text{gcd}(30, 18) = \text{gcd}(18, 12) = \text{gcd}(12, 6) = \text{gcd}(6, 0) = 6$.

Example 2: $a = 3600, b = 1065$.

Once again, we divide 3600 by 1065 with remainder:

$$3600 = 3 \cdot 1065 + 405,$$

replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$$\text{gcd}(3600, 1065) = \text{gcd}(1065, 405) = \text{gcd}(405, 255) = \text{gcd}(255, 150) = \text{gcd}(150, 105) = \text{gcd}(105, 45) = \text{gcd}(45, 15) = \text{gcd}(15, 0) = 15.$$
The Euclidean algorithm in action

**Example 1**: $a = 30, \ b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. 

Math 312, Lecture 4
September 16, 2015
Example 1:  $a = 30, b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$. 
The Euclidean algorithm in action

**Example 1**: $a = 30$, $b = 18$.
Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.
Step 2: Divide 18 by 12.

**Example 2**: $a = 3600$, $b = 1065$.
Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.
$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15$. 
The Euclidean algorithm in action

**Example 1**: $a = 30, \ b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$.

In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$.

**Example 2**: $a = 3600, \ b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15$. 

The Euclidean algorithm in action

**Example 1:** $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

**Example 2:** $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder:

$3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15$.
Example 1: $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$. 

In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$. 

Example 2: $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively. 

$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15$. 

Math 312, Lecture 4
September 16, 2015
The Euclidean algorithm in action

**Example 1**: $a = 30, b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$.

In summary, $\gcd(30, 18) =$
The Euclidean algorithm in action

**Example 1**: $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$.

In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$.

**Example 2**: $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15$. 

In summary, $\gcd(3600, 1065) = 15$. 

Math 312, Lecture 4
September 16, 2015
Example 1: \( a = 30, \ b = 18 \).

Step 1: Divide 30 by 18. \( 30 = 1 \cdot 18 + 12 \). Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \( 18 = 1 \cdot 12 + 6 \). Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \( 12 = 2 \cdot 6 + 0 \). Replace \((12, 6)\) by \((6, 0)\). Now \(\gcd(6, 0) = 6\).

In summary, \(\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \)
Example 1:  \(a = 30, \ b = 18\).

Step 1: Divide 30 by 18. \(30 = 1 \cdot 18 + 12\). Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \(18 = 1 \cdot 12 + 6\). Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \(12 = 2 \cdot 6 + 0\). Replace \((12, 6)\) by \((6, 0)\). Now \(\gcd(6, 0) = 6\).

In summary, \(\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6\).
The Euclidean algorithm in action

**Example 1:** $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\text{gcd}(6, 0) = 6$.

In summary, $\text{gcd}(30, 18) = \text{gcd}(18, 12) = \text{gcd}(12, 6) = \text{gcd}(6, 0) = 6$. 

**Example 2:** $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$\text{gcd}(3600, 1065) = \text{gcd}(1065, 405) = \text{gcd}(405, 255) = \text{gcd}(255, 150) = \text{gcd}(150, 105) = \text{gcd}(105, 45) = \text{gcd}(45, 15) = \text{gcd}(15, 0) = 15$. 

Math 312, Lecture 4
September 16, 2015
The Euclidean algorithm in action

**Example 1:** $a = 30$, $b = 18$.
Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.
Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.
Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$.
In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$.

**Example 2:** $a = 3600$, $b = 1065$.
Once again, we divide 3600 by 1065 with remainder:
The Euclidean algorithm in action

**Example 1**: $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.
Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.
Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\text{gcd}(6, 0) = 6$.

In summary, $\text{gcd}(30, 18) = \text{gcd}(18, 12) = \text{gcd}(12, 6) = \text{gcd}(6, 0) = 6$.

**Example 2**: $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, 
The Euclidean algorithm in action

**Example 1**: $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$.

In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$.

**Example 2**: $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$,
The Euclidean algorithm in action

**Example 1:** \( a = 30, \ b = 18. \)

Step 1: Divide 30 by 18. \( 30 = 1 \cdot 18 + 12. \) Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \( 18 = 1 \cdot 12 + 6. \) Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \( 12 = 2 \cdot 6 + 0. \) Replace \((12, 6)\) by \((6, 0)\). Now \( \gcd(6, 0) = 6. \)

In summary, \( \gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6. \)

**Example 2:** \( a = 3600, \ b = 1065. \)

Once again, we divide 3600 by 1065 with remainder:
\( 3600 = 3 \cdot 1065 + 405, \) replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.
Example 1: $a = 30, \ b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.
Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.
Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\text{gcd}(6, 0) = 6$.

In summary, $\text{gcd}(30, 18) = \text{gcd}(18, 12) = \text{gcd}(12, 6) = \text{gcd}(6, 0) = 6$.

Example 2: $a = 3600, \ b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$\text{gcd}(3600, 1065) =$
The Euclidean algorithm in action

**Example 1:** \( a = 30, \ b = 18. \)

Step 1: Divide 30 by 18. \( 30 = 1 \cdot 18 + 12. \) Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \( 18 = 1 \cdot 12 + 6. \) Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \( 12 = 2 \cdot 6 + 0. \) Replace \((12, 6)\) by \((6, 0)\). Now \( \gcd(6, 0) = 6. \)

In summary, \( \gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6. \)

**Example 2:** \( a = 3600, \ b = 1065. \)

Once again, we divide 3600 by 1065 with remainder: \( 3600 = 3 \cdot 1065 + 405, \) replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.

\( \gcd(3600, 1065) = \gcd(1065, 405) = \)
The Euclidean algorithm in action

**Example 1**: \(a = 30, b = 18\).

Step 1: Divide 30 by 18. \(30 = 1 \cdot 18 + 12\). Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \(18 = 1 \cdot 12 + 6\). Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \(12 = 2 \cdot 6 + 0\). Replace \((12, 6)\) by \((6, 0)\). Now \(\gcd(6, 0) = 6\).

In summary, \(\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6\).

**Example 2**: \(a = 3600, b = 1065\).

Once again, we divide 3600 by 1065 with remainder:
\(3600 = 3 \cdot 1065 + 405\), replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.

\(\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \)
The Euclidean algorithm in action

**Example 1**: \( a = 30, \ b = 18. \)

Step 1: Divide 30 by 18. \( 30 = 1 \cdot 18 + 12. \) Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \( 18 = 1 \cdot 12 + 6. \) Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \( 12 = 2 \cdot 6 + 0. \) Replace \((12, 6)\) by \((6, 0)\). Now \( \gcd(6, 0) = 6. \)

In summary, \( \gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6. \)

**Example 2**: \( a = 3600, \ b = 1065. \)

Once again, we divide 3600 by 1065 with remainder:
\( 3600 = 3 \cdot 1065 + 405, \) replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.

\( \gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \)
The Euclidean algorithm in action

Example 1: \(a = 30, \ b = 18\).

Step 1: Divide 30 by 18. \(30 = 1 \cdot 18 + 12\). Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \(18 = 1 \cdot 12 + 6\). Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \(12 = 2 \cdot 6 + 0\). Replace \((12, 6)\) by \((6, 0)\). Now \(\text{gcd}(6, 0) = 6\).

In summary, \(\text{gcd}(30, 18) = \text{gcd}(18, 12) = \text{gcd}(12, 6) = \text{gcd}(6, 0) = 6\).

Example 2: \(a = 3600, \ b = 1065\).

Once again, we divide 3600 by 1065 with remainder:

\(3600 = 3 \cdot 1065 + 405\), replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.

\(\text{gcd}(3600, 1065) = \text{gcd}(1065, 405) = \text{gcd}(405, 255) = \text{gcd}(255, 150) = \text{gcd}(150, 105) = \)
The Euclidean algorithm in action

**Example 1:** $a = 30$, $b = 18$.

Step 1: Divide 30 by 18. $30 = 1 \cdot 18 + 12$. Replace $(30, 18)$ by $(18, 12)$.

Step 2: Divide 18 by 12. $18 = 1 \cdot 12 + 6$. Replace $(18, 12)$ by $(12, 6)$.

Step 3: Divide 12 by 6. $12 = 2 \cdot 6 + 0$. Replace $(12, 6)$ by $(6, 0)$. Now $\gcd(6, 0) = 6$.

In summary, $\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$.

**Example 2:** $a = 3600$, $b = 1065$.

Once again, we divide 3600 by 1065 with remainder: $3600 = 3 \cdot 1065 + 405$, replace $(3600, 1065)$ by $(1065, 405)$, and proceed recursively.

$$\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) =$$
The Euclidean algorithm in action

**Example 1:** \(a = 30, \ b = 18\).

Step 1: Divide 30 by 18. \(30 = 1 \cdot 18 + 12\). Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \(18 = 1 \cdot 12 + 6\). Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \(12 = 2 \cdot 6 + 0\). Replace \((12, 6)\) by \((6, 0)\). Now \(\text{gcd}(6, 0) = 6\).

In summary, \(\text{gcd}(30, 18) = \text{gcd}(18, 12) = \text{gcd}(12, 6) = \text{gcd}(6, 0) = 6\).

**Example 2:** \(a = 3600, \ b = 1065\).

Once again, we divide 3600 by 1065 with remainder: \(3600 = 3 \cdot 1065 + 405\), replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.

\(\text{gcd}(3600, 1065) = \text{gcd}(1065, 405) = \text{gcd}(405, 255) = \text{gcd}(255, 150) = \text{gcd}(150, 105) = \text{gcd}(105, 45) = \text{gcd}(45, 15) = \)
The Euclidean algorithm in action

**Example 1:** \(a = 30, \ b = 18\).

Step 1: Divide 30 by 18. \(30 = 1 \cdot 18 + 12\). Replace \((30, 18)\) by \((18, 12)\).

Step 2: Divide 18 by 12. \(18 = 1 \cdot 12 + 6\). Replace \((18, 12)\) by \((12, 6)\).

Step 3: Divide 12 by 6. \(12 = 2 \cdot 6 + 0\). Replace \((12, 6)\) by \((6, 0)\). Now \(\gcd(6, 0) = 6\).

In summary, \(\gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6\).

**Example 2:** \(a = 3600, \ b = 1065\).

Once again, we divide 3600 by 1065 with remainder:
\(3600 = 3 \cdot 1065 + 405\), replace \((3600, 1065)\) by \((1065, 405)\), and proceed recursively.

\[\gcd(3600, 1065) = \gcd(1065, 405) = \gcd(405, 255) = \gcd(255, 150) = \gcd(150, 105) = \gcd(105, 45) = \gcd(45, 15) = \gcd(15, 0) = 15.\]
Lemma: Let \( a \geq b > 0 \) be integers. Divide \( a \) by \( b \) with remainder:

\[
a = bq + r, \quad 0 \leq r < b.
\]
Lemma: Let $a \geq b > 0$ be integers. Divide $a$ by $b$ with remainder: 

$$a = bq + r,$$

where $0 \leq r \leq b - 1$. 

Proof: Consider two cases. 

Case 1: $b \leq a$. In this case $r < b \leq a$, as desired. 

Case 2: $b > a$. In this case $q = 1$ and 

$$r = a - bq = a - b > a - a = 0.$$ 

Lemma: Let $a \geq b > 0$ be integers. Divide $a$ by $b$ with remainder:
\[ a = bq + r, \text{ where } 0 \leq r \leq b - 1. \]
Then $r < \frac{1}{2}$. 
Lemma: Let $a \geq b > 0$ be integers. Divide $a$ by $b$ with remainder:

$$a = bq + r,$$

where $0 \leq r \leq b - 1$.

then $r < \frac{1}{2}$.

Proof: Consider two cases.
**Lemma:** Let \( a \geq b > 0 \) be integers. Divide \( a \) by \( b \) with remainder:

\[ a = bq + r, \text{ where } 0 \leq r \leq b - 1. \]

Then \( r < \frac{1}{2} \).

Proof: Consider two cases.

Case 1: \( b \leq \frac{a}{2} \). In this case \( r < b \leq \frac{a}{2} \), as desired.
Lemma: Let \( a \geq b > 0 \) be integers. Divide \( a \) by \( b \) with remainder:
\[
a = bq + r, \text{ where } 0 \leq r \leq b - 1.
\]
Then \( r < \frac{1}{2} \).

Proof: Consider two cases.

Case 1: \( b \leq \frac{a}{2} \). In this case \( r < b \leq \frac{a}{2} \), as desired.

Case 2: \( b > \frac{a}{2} \). In this case \( q = 1 \) and
Lemma: Let $a \geq b > 0$ be integers. Divide $a$ by $b$ with remainder: 
$a = bq + r$, where $0 \leq r \leq b - 1$.

Then $r < \frac{1}{2}$.

Proof: Consider two cases.

Case 1: $b \leq \frac{a}{2}$. In this case $r < b \leq \frac{a}{2}$, as desired.

Case 2: $b > \frac{a}{2}$. In this case $q = 1$ and 

$r = a - qb = a - b > a - \frac{a}{2} = \frac{a}{2}$. 

$\square$
Corollary: Assume $a \geq b > 0$. Then the number of steps required to compute $\gcd(a, b)$
Corollary: Assume $a \geq b > 0$. Then the number of steps required to compute $\gcd(a, b)$ by the Euclidean algorithm is at most $2 \log_2(a)$.

Proof: By the lemma, the larger of the two numbers, $(a, b)$ decreases by at least a factor of 2 after two steps.
Corollary: Assume $a \geq b > 0$. Then the number of steps required to compute $\gcd(a, b)$ by the Euclidean algorithm is at most $2 \log_2(a)$.

Proof: By the lemma, the larger of the two numbers, $(a, b)$ decreases by at least a factor of 2 after two steps. Thus after $2n$ steps this number will be $< \frac{a}{2^n}$. 
Corollary: Assume $a \geq b > 0$. Then the number of steps required to compute $\gcd(a, b)$ by the Euclidean algorithm is at most $2 \log_2(a)$.

Proof: By the lemma, the larger of the two numbers, $(a, b)$ decreases by at least a factor of 2 after two steps.

Thus after $2n$ steps this number will be $< \frac{a}{2^n}$. Since this number is $\geq 1$, the algorithm requires $\geq 2n$ steps only if $2^n < a$, i.e., $n < \log_2(a)$. □