Summary from last unit:

- $\gcd(a, b) =$ greatest common divisor of $a$ and $b$.
- There are integers $s$ and $t$ such that $sa + tb = \gcd(a, b)$.
- Euclidean algorithm efficiently computes $s$, $t$, $\gcd(a, b)$.
There are integers $s$ and $t$ such that $sa + tb = \gcd(a, b)$.

**Warnings:**

- Converse is false: $3 \cdot 6 + 2 \cdot 4 = 26 \neq \gcd(6, 4)$.
- $s, t$ not unique:
  \[ \gcd(6, 4) = 1 \cdot 6 + (-1) \cdot 4 = (-1) \cdot 6 + 2 \cdot 4 \]
Important special case:

If $a$ and $b$ are relatively prime, then there are $u, v$ such that $au + bv = 1$.

And conversely, if $au + bv = 1$ then $a$ and $b$ are relatively prime.
Theorem: Let $n$ be a positive integer and let $b \in \mathbb{Z}_n$. If $\gcd(b, n) = 1$ then there is $v \in \mathbb{Z}_n$ with $bv = 1$.

$v$ is the inverse of $b$ mod $n$.

$v$ is unique (if it exists). $v = b^{-1}$. 
Example: Let $n = 17$, $b = 11$.

$\gcd(11, 17) = 1$. In fact
$-3 \cdot 11 + 2 \cdot 17 = 1$.

Thus $(-3) \% 17 = 14$ is the inverse of 11. Observe
$14 \cdot 11 = 154 \equiv 1 \pmod{17}$ since
$154 = 9 \cdot 17 + 1$. 
Thus, in $\mathbb{Z}_n$, division by $b$ is possible for any $b$ that is relatively prime to $n$.

Example:

Since 8 is relatively prime to 15, 8 has an inverse in $\mathbb{Z}_{15}$: 
$8 \cdot 2 = 1$ in $\mathbb{Z}_{15}$.

$9/8 = 9 \cdot 8^{-1} = 9 \cdot 2 = 3$ in $\mathbb{Z}_{15}$.

$\gcd(10, 15) \neq 1$, so 10 does not have an inverse in $\mathbb{Z}_{15}$. 
The Chinese Remainder Theorem

Let $m_1, m_2 > 0$. Given $a_1, a_2 \in \mathbb{Z}$, when can we simultaneously solve

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}?$$

Answer: if and only if $\gcd(m_1, m_2) = 1$. 
\[
\gcd(m_1, m_2) = 1 \implies u_1 m_1 + u_2 m_2 = 1
\]

Take \( x = a_1 u_2 m_2 + a_2 u_1 m_1 \).

Then \( x \equiv a_i \pmod{m_i} \), for \( i = 1, 2 \).

**Example:** Solve

\[
\begin{align*}
x & \equiv 13 \pmod{100} \\
x & \equiv 5 \pmod{9}
\end{align*}
\]

\[
1 \cdot 100 - 11 \cdot 9 = 1
\]

\[
x = 13(-11)9 + 5 \cdot 1 \cdot 100 = -787 \equiv_{900} 113
\]
Extension:
If \( \gcd(m_i, m_j) = 1 \), for all \( i \neq j \), then for all \( a_1, \ldots, a_k \) there is an \( x \) such that

\[
x \equiv a_i \pmod{m_i} \quad \text{for all } i \leq k.
\]

\( x \) is unique modulo \( m_1 m_2 \cdots m_k \).
Another way to phrase the C.R.T.

Let \( \gcd(r, s) = 1 \).

The function \( f : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s \) given by

\[
f(x) = (x \% r, x \% s)
\]

is a one-to-one correspondence.
Example: \( m_1 = 100, m_2 = 9 \)

\[
 f: \mathbb{Z}_{900} \rightarrow \mathbb{Z}_{100} \times \mathbb{Z}_9; \quad f(x) = (x \mod 100, x \mod 9)
\]

\[
 f(323) = (323 \mod 100, 323 \mod 9) = (23, 8)
\]

To compute the inverse function:

\[
 1 \cdot 100 + (-11) \cdot 9 = 1, \text{ hence } \]

\[
 f^{-1}(a_1, a_2) = (100a_2 - 99a_1) \mod 900.
\]

\[
 f^{-1}(3, 2) = (200 - 297) \mod 900 = 900 - 97 = 803.
\]
\[ \gcd(r, s) = 1 \quad \text{if} \quad f : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s \]

The function \( f \) also preserves addition and multiplication:

\[ f(x + y) = f(x) + f(y) \quad \text{and} \quad f(x \cdot y) = f(x) \cdot f(y). \]

\( f \) is an isomorphism of \( \mathbb{Z}_{rs} \) with \( \mathbb{Z}_r \times \mathbb{Z}_s \).
Example: $r = 4$, $s = 5$ \quad $f: \mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_5$.

$f(7 + 11) = f(18) = (18 \mod 4, 18 \mod 5) = (2, 3)$

$f(7) + f(11) = (3, 2) + (3, 1) = (3 + 3, 2 + 1) = (2, 3)$.

$f(6 \cdot 11) = f(6) = (2, 1)$

$f(6) \cdot f(11) = (2, 1) \cdot (3, 1) = (2 \cdot 3, 1 \cdot 1) = (2, 1)$. 
The Group of Units

\[ \mathbb{Z}_n^* = \{ x \in \mathbb{Z}_n : \gcd(x, n) = 1 \} \quad \text{Units of } \mathbb{Z}_n \]

\[ \phi(n) = |\mathbb{Z}_n^*| \quad \text{Euler totient function} \]

In particular, if \( p \) is prime, then we can divide by any nonzero element of \( \mathbb{Z}_p \), thus

\[ \mathbb{Z}_p^* = \mathbb{Z}_p - \{0\} \text{ and } \phi(p) = p - 1 \]

The group of units is closed under products (see next lecture)
## Multiplication in $\mathbb{Z}_7^*$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Computing $\phi(n)$

We wish to compute $\phi(n) = |\mathbb{Z}_n^*|$. 

$f : \mathbb{Z}_{rs} \rightarrow \mathbb{Z}_r \times \mathbb{Z}_s$, $\gcd(r, s) = 1$. 

$f$ carries invertible elements to invertible elements. Thus, $f$ is also a correspondence $\mathbb{Z}_{rs}^* \rightarrow \mathbb{Z}_r^* \times \mathbb{Z}_s^*$. 

Consequence: if $\gcd(r, s) = 1$, then $\phi(rs) = \phi(r) \cdot \phi(s)$. 

Suppose the prime factorization of $n$ is $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. 

Then $\phi(n) = \phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$. 

© 2011 Clifford Bergman
If $p$ is prime, what is $\phi(p^e)$?

Which numbers are not relatively prime to $p^e$?

Answer: $p, 2p, 3p, \ldots, p^{e-1} \cdot p$

Thus $\phi(p^e) = p^e - p^{e-1}$

$= p^{e-1}(p - 1)$

$= p^e \left(1 - \frac{1}{p}\right)$. 

© 2011 Clifford Bergman
Theorem: if \( n = p_1^{e_1} \cdots p_k^{e_k} \) then

\[
\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k})
= p_1^{e_1-1}(p_1 - 1) \cdots p_k^{e_k-1}(p_k - 1)
= n \cdot (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k).
\]

Example: \( \phi(200) = \phi(2^3) \cdot \phi(5^2) = 2^2(2 - 1) \cdot 5^1(5 - 1) = 80 \)