Number Theory and Modular Arithmetic

Lecture 13 (October 06, 2008)

$\equiv_p 1$

MAX(a,b) + MIN(a,b) = a+b

$n|m$ means that $m$ is an integer multiple of $n$.
We say that “$n$ divides $m$”.

Greatest Common Divisor:
$GCD(x,y) =$ greatest $k \geq 1$ s.t. $k|x$ and $k|y$.

Least Common Multiple:
$LCM(x,y) =$ smallest $k \geq 1$ s.t. $x|k$ and $y|k$.

Fact:
$GCD(x,y) \times LCM(x,y) = x \times y$

You can use $MAX(a,b) + MIN(a,b) = a+b$ to prove the above fact...
(a mod n) means the remainder when a is divided by n.

If \( a = dn + r \) with \( 0 \leq r < n \)
Then \( r = (a \mod n) \)
and \( d = (a \div n) \)

\( a \equiv b \mod n \)

\( a \equiv b \mod n \)

\( a = b \mod n \)

\( \Leftrightarrow (a \mod n) = (b \mod n) \)

\( \Leftrightarrow n|(a-b) \)

Written as \( a \equiv b \mod n \)

“a and b are equivalent modulo n”

\( 31 \equiv 81 \mod 2 \)

\( 31 \equiv 81 \)

\( \equiv \) is an equivalence relation

In other words, it is

Reflexive:
\( a \equiv a \)

Symmetric:
\( (a \equiv b) \Rightarrow (b \equiv a) \)

Transitive:
\( (a \equiv b \text{ and } b \equiv c) \Rightarrow (a \equiv c) \)

\( a \equiv b \Leftrightarrow n|(a-b) \)

“a and b are equivalent modulo n”

\( a \equiv b \mod n \)

\( a \equiv b \mod n \)

defines a natural partition of the integers into \( n \) classes.

a and b are said to be in the same “residue class” or “congruence class” precisely when \( a \equiv b \mod n \).

Residue Classes Mod 3:

\[[0] = \{..., -6, -3, 0, 3, 6, ..\} \]
\[[1] = \{..., -5, -2, 1, 4, 7, ..\} \]
\[[2] = \{..., -4, -1, 2, 5, 8, ..\} \]
\[[3] = \{..., -6, -3, 0, 3, 6, ..\} \]
\[[6] = \{..., -4, -1, 2, 5, 8, ..\} \]
\[[7] = \{..., -5, -2, 1, 4, 7, ..\} \]
\[[10] = \{..., -6, -3, 0, 3, 6, ..\} \]
Fact: equivalence mod $n$ implies equivalence mod any divisor of $n$.

If $(x \equiv_n y)$ and $(k|n)$
Then: $x \equiv_k y$

Example: $10 \equiv_6 16 \implies 10 \equiv_3 16$

If $(x \equiv_n y)$ and $(k|n)$
then $x \equiv_k y$

Proof: $\frac{n}{k} \cdot \frac{x}{y}$
$\implies \frac{k}{x} \cdot \frac{y}{y}$
$\implies x \equiv_k y$

Proof of 3: $xa = yb \pmod{n}$
(The other two proofs are similar…)

Fundamental lemma of plus, minus, and times mod $n$:

If $(x \equiv_n y)$ and $(a \equiv_n b)$. Then
1) $x + a \equiv_n y + b$
2) $x - a \equiv_n y - b$
3) $x \cdot a \equiv_n y \cdot b$

Fundamental lemma of plus minus, and times modulo $n$:

When doing plus, minus, and times modulo $n$, I can at any time in the calculation replace a number with a number in the same residue class modulo $n$

Please calculate:

$$249 \cdot 504 \mod 251$$

when working mod 251

$-2 \cdot 2 = -4 = 247$
A Unique Representation System Modulo $n$:

We pick exactly one representative from each residue class.

We do all our calculations using these representatives.

Unique representation system modulo 3

Finite set $S = \{0, 1, 2\}$

+ and * defined on $S$:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Perhaps the most convenient set of representatives:

The reduced system modulo $n$:

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Define operations $+_n$ and $*_n$:

$a *_n b = (a*b \mod n)$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a +_n b = (a+b \mod n)$

$["Closed"]$

$x, y \in Z_n \Rightarrow x +_n y \in Z_n$

$["Associative"]$

$x, y, z \in Z_n \Rightarrow (x +_n y) +_n z = x +_n (y +_n z)$

$["Commutative"]$

$x, y \in Z_n \Rightarrow x +_n y = y +_n x$
$Z_n = \{0, 1, 2, \ldots, n-1\}$

$+\_n b = (a+b \mod n)$

$a *\_n b = (a*b \mod n)$

$+\_n$ and $*\_n$ are commutative and associative binary operators from $Z_n \times Z_n \rightarrow Z_n$

The reduced system modulo 3

$Z_3 = \{0, 1, 2\}$

Two binary, associative operators on $Z_3$:

<table>
<thead>
<tr>
<th>+_3</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>*_3</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The reduced system modulo 2

$Z_2 = \{0, 1\}$

Two binary, associative operators on $Z_2$:

<table>
<thead>
<tr>
<th>+_2</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>*_2</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

The Boolean interpretation of $Z_2$

$Z_2 = \{0, 1\}$

Two binary, associative operators on $Z_2$:

<table>
<thead>
<tr>
<th>+_2 XOR</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>*_2 AND</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The reduced system

$Z_4 = \{0, 1, 2, 3\}$

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 3 | 0 | 3 | 2 |

The reduced system

$Z_5 = \{0, 1, 2, 3, 4\}$

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 0 | 1 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| * | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |
An operator has the permutation property if each row and each column has a permutation of the elements.

For every $n$, $\oplus_n$ on $\mathbb{Z}_n$ has the permutation property.

What about multiplication? Does $\ast_6$ on $\mathbb{Z}_6$ have the permutation property? No

What about $\ast_8$ on $\mathbb{Z}_8$?

A visual way to understand multiplication and the "permutation property".
The multiples of $c$ modulo $n$ is the set:
\[ \{0, c, c+n, c+2n, c+3n, \ldots \} \]
\[ = \{kc \mod n \mid 0 \leq k \leq n-1 \} \]

There are exactly 8 distinct multiples of 3 modulo 8.
hit all numbers ⇔ row 3 has the “permutation property”

There are exactly 2 distinct multiples of 4 modulo 8
row 4 does not have “permutation property” for * on $\mathbb{Z}_8$

There is exactly 1 distinct multiple of 8 modulo 8

What’s the pattern?

- exactly 8 distinct multiples of 3 modulo 8.
- exactly 2 distinct multiples of 4 modulo 8
- exactly 1 distinct multiple of 8 modulo 8
- exactly 4 distinct multiples of 6 modulo 8

exactly \( \frac{\phi(n)}{n} \) distinct multiple of $x$ modulo $y$
There are exactly \( \text{LCM}(n,c)/c = n/\text{GCD}(c,n) \) distinct multiples of \( c \) modulo \( n \).

Hence, only those values of \( c \) with \( \text{GCD}(c,n) = 1 \) have the permutation property for \( \ast \) modulo \( n \). (that is, they have \( n \) distinct multiples modulo \( n \)).

Theorem: There are exactly \( k = n/\text{GCD}(c,n) \) distinct multiples of \( c \) modulo \( n \), and these multiples are \( \{ c \cdot i \mod n \mid 0 \leq i < k \} \).

Proof:
Clearly, \( c/\text{GCD}(c,n) \geq 1 \) is a whole number.

\( ck = n/\text{GCD}(c,n) = n(c/\text{GCD}(c,n)) \equiv 0 \mod n \)

\( \Rightarrow \) There are \( \leq k \) distinct multiples of \( c \mod n \): \( c^0, c^1, c^2, \ldots, c^{(k-1)} \)

\( \Rightarrow \) Also, \( k \) is all the factors of \( n \) missing from \( c \)

\( \Rightarrow cx \equiv_n cy \Rightarrow n(c(x-y)) \Rightarrow k(x-y) \Rightarrow x-y \geq k \)

\( \Rightarrow \) There are \( \geq k \) multiples of \( c \). Hence exactly \( k \).

So, if we write the addition and multiplication tables for \( Z_n \)...
Is there a fundamental lemma of division modulo \( n \)?

\[
\text{If } c \equiv 0 \pmod{n}, \text{ then } cx \equiv n cy \text{ for all } x \text{ and } y.
\]

Canceling the \( c \) is like dividing by zero.

**Let’s fix that!**

Repaired fundamental lemma of division modulo \( n \):

\[
\text{if } c \not\equiv 0 \pmod{n}, \text{ then } cx \equiv n cy \Rightarrow x \equiv n y.
\]

\( 6 \equiv 3 \pmod{10} \), but not \( 3 \equiv 8 \).

\( 2 \equiv 5 \pmod{6} \), but not \( 2 \equiv 5 \).

When can’t I divide by \( c \)?

Theorem: There are exactly \( n/\gcd(c,n) \) distinct multiples of \( c \) modulo \( n \).

Corollary: If \( \gcd(c,n) > 1 \), then the number of multiples of \( c \) is less than \( n \).

Corollary: If \( \gcd(c,n) > 1 \) then you can’t always divide by \( c \).

Proof: There must exist distinct \( x, y < n \) such that \( c \cdot x = c \cdot y \) (but \( x \neq y \)). Hence can’t divide.

Fundamental lemma of division modulo \( n \):

\[
\text{if } \gcd(c,n) = 1, \text{ then } ca \equiv cb \Rightarrow a \equiv b \text{.}
\]

Proof:

\[
\begin{align*}
\text{Let } & n \mid cx - cy \\
\text{and } & \gcd(x,y) = 1 \\
\Rightarrow & n \mid x - y \text{, i.e. } x \equiv y \\
\end{align*}
\]

Corollary for general \( c \):

\[
\text{if } \gcd(c,n) = 1, \text{ then } x \equiv y \pmod{\frac{n}{\gcd(c,n)}}
\]
Fundamental lemma of division modulo n.
If $\text{GCD}(c,n)=1$, then $ca \equiv_n cb \Rightarrow a \equiv_n b$

Consider the set
$Z_n^* = \{x \in \mathbb{Z}_n | \text{GCD}(x,n) = 1\}$

Multiplication over this set $Z_n^*$ will have the cancellation property.

What are the properties of $Z_n^*$

For $\ast_n$ on $\mathbb{Z}_n$ we showed the following properties:

[Closure] $x, y \in \mathbb{Z}_n \Rightarrow x \ast_n y \in \mathbb{Z}_n$

[Associativity] $x, y, z \in \mathbb{Z}_n \Rightarrow (x \ast_n y) \ast_n z = x \ast_n (y \ast_n z)$

[Commutativity] $x, y \in \mathbb{Z}_n \Rightarrow x \ast_n y = y \ast_n x$

What about $\ast_n$ on $Z_n^*$?

All these 3 properties hold for $\ast_n$ on $Z_n^*$.

Let’s show “closure”: $x, y \in Z_n^* \Rightarrow x \ast_n y \in Z_n^*$

Formal Proof:
Let $z = xy$. Let $z' = z \mod n$. Then $z = z' + kn$.
Suppose $z'$ not in $Z_n^*$. Then $\text{GCD}(z', n) > 1$.
and hence $\text{GCD}(z, n) > 1$.
Hence there exists a prime $p > 1$ s.t. $p|z'$ and $p|n$.
$p|z \Rightarrow p|x$ or $p|y$. (say $p|x$)
Hence $p|n$, so $\text{GCD}(x, n) > 1$.
Contradiction of $x \in Z_n^*$. 

$Z_{12}^* = \{0 \leq x < 12 \mid \text{gcd}(x,12) = 1\}
= \{1, 5, 7, 11\}$ 

<table>
<thead>
<tr>
<th>$\ast_{12}$</th>
<th>1</th>
<th>5</th>
<th>7</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>
Fact:
For prime $p$, the set $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

Proof:
It just follows from the definition!

For a prime, all $0 < x < p$ satisfy $\gcd(x, p) = 1$

Euler Phi Function $\phi(n)$

Define $\phi(n) =$ size of $\mathbb{Z}_n^*$ = number of $1 \leq k < n$ that are relatively prime to $n$.

$p$ prime $\Rightarrow \mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$
$\Rightarrow \phi(p) = p-1$

Theorem: if $p, q$ distinct primes then $\phi(pq) = (p-1)(q-1)$

How about $p = 3, q = 5$?

$\phi(12) = 4$
Theorem: if \( p, q \) distinct primes then
\[
\phi(pq) = (p-1)(q-1)
\]

\( pq \) = # of numbers from 1 to \( pq \)
\( p \) = # of multiples of \( q \) up to \( pq \)
\( q \) = # of multiples of \( p \) up to \( pq \)
\( 1 \) = # of multiple of both \( p \) and \( q \) up to \( pq \)

\[ \phi(pq) = pq - p - q + 1 = (p-1)(q-1) \]

Additive and Multiplicative Inverses

The additive inverse of \( a \in \mathbb{Z}_n \) is the unique \( b \in \mathbb{Z}_n \) such that
\[ a +_n b \equiv_n 0. \]
We denote this inverse by “\(-a\)”. It is trivial to calculate: “\(-a\)” = \((n-a)\).

The multiplicative inverse of \( a \in \mathbb{Z}_n^* \) is the unique \( b \in \mathbb{Z}_n^* \) such that
\[ a *_n b =_n 1. \]
We denote this inverse by “\(a^{-1}\)” or “\(1/a\)”. The unique inverse of “\(a\)” must exist because the “\(a\)” row contains a permutation of the elements and hence contains a unique 1.

What is the additive inverse of
\[ a = 342952340 \]
in
\[ \mathbb{Z}_{4230493243} = \mathbb{Z}_n^? \]
Answer: \( n - a = 3887540903 \)

What is the multiplicative inverse of
\[ 342952340 \]
in
\[ \mathbb{Z}_{4230493243}^* =? \]
Answer: 583739113
How do you find multiplicative inverses fast?

**Euclid’s Algorithm for GCD**

<table>
<thead>
<tr>
<th>Euclid(A, B)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If B=0 then return A</td>
<td></td>
</tr>
<tr>
<td>else return Euclid(B, A mod B)</td>
<td></td>
</tr>
</tbody>
</table>

| Euclid(67, 29) | 67 – 2*29 = 67 mod 29 = 9 |
| Euclid(29, 9) | 29 – 3*9 = 29 mod 9 = 2 |
| Euclid(9, 2) | 9 – 4*2 = 9 mod 2 = 1 |
| Euclid(2, 1) | 2 – 2*1 = 2 mod 1 = 0 |
| Euclid(1, 0) outputs 1 |

**Extended Euclid Algorithm**

Not only does it output GCD(A, B) it also outputs integers r, s such that

\[ rA + sB = \text{GCD}(A, B) \]

**Efficient algorithm to compute a\(^{-1}\) from a and n.**

Run Extended Euclidean Algorithm on the numbers a and n.

It will give two integers r and s such that \( ra + sn = \text{gcd}(a, n) = 1 \)

Taking both sides modulo n, we obtain: \( ra \equiv 1 \) (mod n)

Output r, which is the inverse of a

**Example**

Multiplicative inverse of 29 in \( \mathbb{Z}_{67}^+ \) ?

\[ 1 = 13\cdot67 - 30\cdot29 \]

Hence: \( 29^{-1} = -30 = 37 \mod 67 \)
Z_n = \{0, 1, 2, ..., n-1\}
Z_n^* = \{x \in Z_n \mid \gcd(x,n) = 1\}

Define +, and *:
\[ a +_n b = (a+b \mod n) \]
\[ a *_n b = (a*b \mod n) \]

\(<Z_n^+, > >
1. Closed
2. Associative
3. 0 is identity
4. Multiplicative Inverses
5. Cancellation
6. Commutative
\[ c *_n (a +_n b) \equiv (c *_n a) +_n (c *_n b) \]

\(<Z_n^*, > >
1. Closed
2. Associative
3. 1 is identity
4. Additive Inverses
5. Cancellation
6. Commutative

Euler Phi Function
\[ \phi(n) = \text{size of } Z_n^* \]

p prime \(\Rightarrow Z_p^* = \{1, 2, 3, ..., p-1\} \)
\[ \Rightarrow \phi(p) = p-1 \]

\[ \phi(pq) = (p-1)(q-1) \]
if p, q distinct primes

Working modulo integer n
Definitions of \( Z_n, Z_n^* \) and their properties
Fundamental lemmas of +, -, *, /
When can you divide out
How to calculate \( c^{-1} \mod n \).

Euler phi function \( \phi(n) = |Z_n^*| \)

Here’s What You Need to Know…