Numb3rs

Lecture 6
Modular Arithmetic
And More Intriguing Structures
Story So Far

- Quotient and Remainder
- GCD
  - Euclid's algorithm to compute gcd(a,b)
  - \( L(a,b) \triangleq \{ au + bv \mid u,v \in \mathbb{Z} \} \)
  - \( = \{ n \cdot \gcd(a,b) \mid n \in \mathbb{Z} \} \)
- Primes
- Fundamental Theorem of Arithmetic

Modular Arithmetic (\(\mathbb{Z}_m\))

- Addition and Multiplication
- Multiplicative Inverse!

- \(\gcd(a,m)=1 \iff \exists u,v \ au + mv = 1 \iff \exists u \ [a]_m \times_m [u]_m = [1]_m \)
- For prime \(p\), every element in \(\mathbb{Z}_p\setminus\{0\}\) has mult. inverse
Suppose $d|\text{m}$. Consider the two statements:

I. $\forall a, b\ a \equiv b \pmod{m} \rightarrow a \equiv b \pmod{d}$

II. $\forall a, b\ a \equiv b \pmod{d} \rightarrow a \equiv b \pmod{m}$

A. Both I & II are true
B. I is true, II is false
C. I is false, II is true
D. Both I & II are false
Chiming Clocks

Two clocks, with a hours and b hours on their dials
Say they both start at 0, and move one step every minute
  e.g., a=13, b=9. After 3 minutes, both point to 3. After 10 minutes, the first clock points to 10, and the second to 1.
Each clock has a position where it chimes, say r and s, respectively
  e.g., r=11 and s=5

Question: Will the two clocks ever chime together?
An Example

Say, \(a=3\) and \(b=5\)

Note that after \(\text{lcm}(a,b) = 15\) steps, both clocks will be back to 0

So enough to check the first 15 steps

Let’s find out all pairs \((r,s)\) that the two clocks will simultaneously reach

All 15 possible pairs occur, once each!
As Modular Arithmetic

Consider mapping elements in $\mathbb{Z}_{15}$ (all 15 of them) to $\mathbb{Z}_3$ and $\mathbb{Z}_5$

$\mapsto (x \mod 3, x \mod 5)$

All 15 possible pairs occur, once each

That is, for each $(r,s) \in \mathbb{Z}_3 \times \mathbb{Z}_5$, there is exactly one $x$ such that

$x \equiv r \pmod{3}$ and $x \equiv s \pmod{5}$

For which $a,b$ are we guaranteed that there is a solution for this system (no matter what $r,s$ is)?

<table>
<thead>
<tr>
<th>$\mathbb{Z}_{15}$</th>
<th>$\mathbb{Z}_3$</th>
<th>$\mathbb{Z}_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>
Chinese Remainder Theorem

If \( \gcd(a,b) = 1 \), then for all \((r,s)\) there is a unique solution (modulo \(ab\)) to the system

\[
x \equiv r \pmod{a} \quad \text{and} \quad x \equiv s \pmod{b}
\]

Proof of existence:

Will solve for \((r,s) = (1,0)\) and for \((r,s) = (0,1)\)

i.e., \( \alpha \equiv 1 \pmod{a}, \alpha \equiv 0 \pmod{b} \),
\( \beta \equiv 0 \pmod{a}, \beta \equiv 1 \pmod{b} \),

Then, can let \( x = \alpha r + \beta s \).

\( \exists \ u, v \ \ \ au + bv = 1 \) (can compute using EEA)

Let \( \alpha = 1 - au = bv \) and \( \beta = 1 - bv = au \)
**Chinese Remainder Theorem**

If \( \gcd(a,b) = 1 \), then for all \((r,s)\) there is a unique solution (modulo \(ab\)) to the system

\[
x \equiv r \pmod{a} \quad \text{and} \quad x \equiv s \pmod{b}
\]

**Existence:** \( x = bvr + aus \), where \( au+bv=1 \)

**Uniqueness:**
- There are only \( ab \) possible values of \( x \)
- There are \( ab \) pairs \((r,s)\)
- Each \( x \) is a solution for exactly one \((r,s)\)
- Every pair \((r,s)\) has at least one solution
- Hence, no pair \((r,s)\) has two solutions
Chinese Remainder Theorem

If \( \gcd(a,b) = 1 \), then for all \((r,s)\) there is a unique solution (modulo \(ab\)) to the system
\[
x \equiv r \pmod{a} \quad \text{and} \quad x \equiv s \pmod{b}
\]

Existence: \( x = bvr + aus \), where \( au+bv=1 \)

Uniqueness: \( |\mathbb{Z}_{ab}| = |\mathbb{Z}_a| \cdot |\mathbb{Z}_b| \)

**CRT Representation:**

- Represent \( x \in \mathbb{Z}_{ab} \) as the pair \((r,s) = (\text{rem}(x,a), \text{rem}(x,b)) \in \mathbb{Z}_a \times \mathbb{Z}_b\)
- Can go back from \((r,s)\) to \(x\) uniquely, using EEA

<table>
<thead>
<tr>
<th>( \mathbb{Z}_{15} )</th>
<th>( \mathbb{Z}_3 )</th>
<th>( \mathbb{Z}_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>
Suppose \( m = ab \), where \( \gcd(a,b) = 1 \)

Can use CRT representation to do arithmetic in \( \mathbb{Z}_m \) using arithmetic in \( \mathbb{Z}_a \) and \( \mathbb{Z}_b \)

CRT representation of \( \mathbb{Z}_m \): every element of \( \mathbb{Z}_m \) can be written as a unique element of \( \mathbb{Z}_a \times \mathbb{Z}_b \)

Addition and multiplication can be done coordinate-wise in CRT representation

- If \( \text{rem}(x,a) = r \) and \( \text{rem}(x',a) = r' \), then \( \text{rem}(x+x',a) \equiv r + r' \pmod{a} \). Similarly, \( \text{mod} b \).
- \( (r, s) +_m (r', s') = (r +_a r', s +_b s') \)
- Similarly, \( (r, s) \times_m (r', s') = (r \times_a r', s \times_b s') \)
CRT and Inverses

- Addition and multiplication can be done coordinate-wise in CRT representation
- Additive identity is (0,0) and multiplicative identity is (1,1)
- Additive and multiplicative inverses are coordinate-wise too
  - \((r,s) +_{(m)} (r',s') = (0,0) \iff r +_{(a)} r' = 0, \ s +_{(b)} s' = 0\)
  - \((r,s) \times_{(m)} (r',s') = (1,1) \iff r \times_{(a)} r' = 1, \ s \times_{(b)} s' = 1\)

\[
\begin{array}{|c|c|c|}
\hline
Z_{15} & Z_3 & Z_5 \\
\hline
0 & 0 & 0 \\
1 & 1 & 1 \\
2 & 2 & 2 \\
3 & 0 & 3 \\
4 & 1 & 4 \\
5 & 2 & 0 \\
6 & 0 & 1 \\
7 & 1 & 2 \\
8 & 2 & 3 \\
9 & 0 & 4 \\
10 & 1 & 0 \\
11 & 2 & 1 \\
12 & 0 & 2 \\
13 & 1 & 3 \\
14 & 2 & 4 \\
\hline
\end{array}
\]
CRT and Inverses

Addition and multiplication can be done coordinate-wise in CRT representation.

- **Additive identity** is (0,0) and **multiplicative identity** is (1,1).

- **Additive and multiplicative inverses** are coordinate-wise too.

\[(r,s) +_{(m)} (r',s') = (0,0) \iff r +_{(a)} r' = 0, \quad s +_{(b)} s' = 0\]

\[(r,s) \times_{(m)} (r',s') = (1,1) \iff r \times_{(a)} r' = 1, \quad s \times_{(b)} s' = 1\]

- **x** has multiplicative inverse modulo **m** iff it has multiplicative inverses modulo **a** and **b**

\[\gcd(x,m)=1 \iff \gcd(x,a)=1 \text{ and } \gcd(x,b)=1\]

\[m = ab, \text{ where } \gcd(a,b) = 1\]
CRT Beyond 2 Factors

Suppose \( m = a_1 \cdot a_2 \cdot \ldots \cdot a_n \), where \( \gcd(a_i,a_j)=1 \) for all \( i \neq j \). For any \( (r_1,\ldots,r_n) \) with \( r_i \in \mathbb{Z}_{a_i} \) for each \( i \), there is a unique solution in \( \mathbb{Z}_n \) for the system of congruences \( x \equiv r_i \pmod{a_i} \) for \( i=1,\ldots,n \)

Proof by (weak) induction:

- **Base case:** \( n=1 \) ✓
- **Induction step:** We shall prove that for all \( k \geq 1 \), (induction hypothesis) if every system of \( k \) congruences with co-prime moduli has a unique solution, (to prove) then so does every such system of \( k+1 \) congruences.

Given \( (a_1,\ldots,a_{k+1},r_1,\ldots,r_{k+1}) \), define a system for \( (a_1,\ldots,a_k,r_1,\ldots,r_k) \), get its unique solution, say \( s \). Define a system of 2 congruences, with co-prime moduli \( a = a_1 \cdot \ldots \cdot a_k \), and \( b=a_{k+1} \),

\[
x \equiv s \pmod{a} \quad \text{and} \quad x \equiv r_{k+1} \pmod{a_{k+1}}.
\]

By CRT, this has a unique solution. This is the unique solution for the original system (why?).
Multiplicative Inverses, Again

- Recall: a has a multiplicative inverse in \( \mathbb{Z}_m \) iff \( \gcd(a, m) = 1 \)
  - Such an element is called a *unit* of \( \mathbb{Z}_m \)

**How many units are there in \( \mathbb{Z}_m \)?**

- When \( m \) is prime? \( m - 1 \) (all except 0)
- When \( m = p^2 \), where \( p \) is prime?
  - A common factor with \( p^2 \) iff a multiple of \( p \) (in \( \{0, p, 2p, \ldots, (p-1)p\} \) )
  - i.e., \( p^2 - p \)
- When \( m = p^k \), where \( p \) is prime? \( p^k - p^{k-1} = m(1 - 1/p) \)
- When \( m = p_1^{d_1} \cdots p_n^{d_n} \) where \( p_i \) are primes?
  - By CRT, elements of the form \( (r_1, \ldots, r_n) \), where each \( r_i \) is invertible modulo \( p_i^{d_i} \)
  - \( \Pi_i p_i^{d_i} (1 - 1/p_i) = m(1 - 1/p_1) \cdots (1 - 1/p_n) \)
Multiplicative Inverses, Again

How many units are there in \( \mathbb{Z}_m \)?

\[ \varphi(m) = m \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right) \]

where \( p_1, \ldots, p_n \) are the prime factors of \( m \)

Euler's \( \varphi \) function (a.k.a. Euler's totient function)

If \( \text{gcd}(a,b) = 1 \), then \( \varphi(ab) = \varphi(a) \cdot \varphi(b) \)

Such a function is called a multipliciative function
Multiplicative Inverses, Again

Examples

- $m=6$
  - $\varphi(6) = (2-1)(3-1) = 2$
  - $\mathbb{Z}_6^* = \{1, 5\}$

- $m=10$
  - $\varphi(10) = (2-1)(5-1) = 4$
  - $\mathbb{Z}_{10}^* = \{1,3,7,9\}$

Note: The multiplication table restricted to units only has units!

Why?
The Units, $\mathbb{Z}_m^*$

- If $a \in \mathbb{Z}_m \setminus \mathbb{Z}_m^*$ then $\exists u \neq 0$ s.t. $au = 0$ in $\mathbb{Z}_m$
  - $a$ not unit $\Rightarrow \gcd(a, m) > 1 \Rightarrow m/\gcd(a, m) < m$
    $\Rightarrow \exists u$ (namely $m/\gcd(a, m)$) s.t. $0 < u < m$, $au = 0$ in $\mathbb{Z}_m$

- Converse also holds:
  - Suppose $\exists u \neq 0$, $au = 0$ and $ba = 1$. Then $0 = b0 = bau = 1u = u$

- $a \in \mathbb{Z}_m^* \rightarrow a^{-1} \in \mathbb{Z}_m^*$

- $a, b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$, because $(ab)(b^{-1}a^{-1}) = 1$

- For each $a \in \mathbb{Z}_m^*$, $a \cdot \mathbb{Z}_m^* \triangleq \{ ab \mid b \in \mathbb{Z}_m^* \} = \mathbb{Z}_m^*$
  - Since $a, b \in \mathbb{Z}_m^* \rightarrow ab \in \mathbb{Z}_m^*$, we have $a \cdot \mathbb{Z}_m^* \subseteq \mathbb{Z}_m^*$
  - $\forall x \in \mathbb{Z}_m^*$ we have $a^{-1}x \in \mathbb{Z}_m^*$ (why?) $\Rightarrow x \in a \cdot \mathbb{Z}_m^*$. Hence $\mathbb{Z}_m^* \subseteq a \cdot \mathbb{Z}_m^*$
  - So $a \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^*$ (the row for $a$ in the multiplication table restricted to $\mathbb{Z}_m^*$ has exactly all the elements in $\mathbb{Z}_m^*$)
Euler’s Totient Theorem

\[ \forall a \in \mathbb{Z}_m^*, \ a^{\phi(m)} \equiv 1 \pmod{m} \]

Proof: Fix any \( m \) and \( a \in \mathbb{Z}_m^* \).

Let \( \mathbb{Z}_m^* = \{x_1, \ldots, x_n\} \) where \( n = \phi(m) \).

Let \( u = x_1 \ldots x_n \) and \( w = (a \cdot x_1) \cdot \ldots \cdot (a \cdot x_n) \).

\[ \Rightarrow w = a^n \cdot u. \]

But also, \( w = \prod_{x \in a \mathbb{Z}_m^*} x = \prod_{x \in \mathbb{Z}_m^*} x = u \) (because \( a \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^* \))

\[ \Rightarrow u = a^n \cdot u, \text{ where } u \in \mathbb{Z}_m^* \]

\[ \Rightarrow 1 = a^n \text{ by multiplying both sides with } u^{-1} \]

Special case, when \( m \) is a prime

**Fermat’s Little Theorem:**

For prime \( p \) and \( a \) not a multiple of \( p \), \( a^{p-1} \equiv 1 \pmod{p} \)