Lecture 8  Modular Arithmetic (continued)

[Finish previous notes, then:]

\[ \mathbb{Z}_n \text{ has operations } + \text{ and } \cdot : [a] + [b] = [a+b] \]
\[ [a] \cdot [b] = [a \cdot b] \]

A **multiplicative inverse** for \([a] \in \mathbb{Z}_n \) is \([b] \in \mathbb{Z}_n \) such that \([a] \cdot [b] = [1] \).

**Proposition (19.9)** For \( n \geq 2 \), \([a] \in \mathbb{Z}_n \) has a multiplicative inverse if and only if \( \gcd(a,n) = 1 \).

**Proof**: Suppose there is \([b] \in \mathbb{Z}_n \) such that \([a] \cdot [b] = [1] \)
then \([ab] = [1] \) so \( ab \equiv 1 \pmod{n} \) so \( n \mid (1-ab) \) so \( 1-ab = tn \) for some \( t \in \mathbb{Z} \).

Thus \( ab + tn = 1 \). If \( d \mid a \) and \( d \mid n \), then \( d \mid ab + tn \), so \( d \mid 1 \) and so \( d = \pm 1 \). Thus \( \gcd(a,n) = 1 \).

Conversely, suppose \( \gcd(a,n) = 1 \). Then we can find \( b,t \) such that \( ab + tn = 1 \). Then \( 1-ab = tn \)
so \( n \mid (1-ab) \) so \( ab \equiv 1 \pmod{n} \) so \([ab] = [1] \) so \([a] \cdot [b] = [1] \) and \([b] \) is a multiplicative inverse to \([a] \). \( \blacksquare \)

Set \( \mathbb{Z}_n^x = \{ [a] \mid \gcd(a,n) = 1 \} \leq \mathbb{Z}_n \)
Denote by \( [a]^{-1} \) the multiplicative inverse for \([a] \in \mathbb{Z}_n^x \)

**Examples**: \( \mathbb{Z}_{12}^x = \{ [1], [5], [7], [11] \} \leq \mathbb{Z}_{12} \)
\( \mathbb{Z}_7^x = \{ [1], [2], [3], [4], [5], [6] \} \leq \mathbb{Z}_7 \)
Proposition: \( (\mathbb{Z}_n^*, \cdot) \) is a commutative group.

Proof: Need check that the set \( \mathbb{Z}_n^* \) is closed under multiplication and taking of inverses.

Let \([a][b] \in \mathbb{Z}_n^*\). Pick inverses \([a]^{-1}\) and \([b]^{-1}\).

Then \(([a][b])([a]^{-1}[b]^{-1}) = [a][a]^{-1}[b][b]^{-1} = \langle 1 \rangle \cdot \langle 1 \rangle = \langle 1 \rangle\)

so \([a]^{-1}[b]^{-1}\) is a multiplicative inverse of \([a][b]\), and

so \([a]^{-1}[b] \in \mathbb{Z}_n^*\).

So multiplication is a function \( \mathbb{Z}_n^* \times \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^* \)

Associativity has already been checked.

Identity: indeed \([1] \in \mathbb{Z}_n^*\) since \(\gcd(1, n) = 1\), and we already know \([1] \cdot [a] = [a]\)

Inverses: if \([a] \in \mathbb{Z}_n^*\), \([a]^{-1} [a] = \langle 1 \rangle\), so \([a]^{-1}\) is an inverse of \([a]^{-1}\) and so \([a]^{-1} \in \mathbb{Z}_n^*\) as well. So \(\mathbb{Z}_n^*\)

has inverses.

Commutativity is also clear. \(\square\)

Zero divisors: \([0] \in \mathbb{Z}_n\) such that \([a] \neq [0]\) but there is \([b] \in \mathbb{Z}_n^* \), \([b] \neq [0]\), such that \([a][b] = [0]\).

On homework will show that \([a]\) is a zero divisor iff

\([a] \in \mathbb{Z}_n^*\) and \([a] \neq [0]\).

We will finish (for now) our discussion of modular arithmetic with an ancient theorem.

Lemma: (Cor. 1.6.17) Let \(a\) and \(b\) be relatively prime natural numbers, and let \(x\) be an integer. If \(a \mid x\) and \(b \mid x\) then \(ab \mid x\).

Proof: Since \(\gcd(a,b) = 1\), we can write \(sa + tb = 1\) for some integers \(s\) and \(t\).
Then \( x = sax + tbx \)
Since \( a \mid x \), we can write \( x = aq \) \( (q \in \mathbb{Z}) \)
Since \( b \mid x \), we can write \( x = br \) \( (r \in \mathbb{Z}) \)
So \( x = sax + t bx \)
\[ = sabr + t baq \]
\[ = (sr + tqr)ab \]
So \( ab \mid x \).

**Chinese remainder theorem (c. 300 ??? C.E.)**

Let \( a \) and \( b \) be relatively prime natural numbers.
Let \( \alpha \) and \( \beta \) be an integers. Then there exists a solution \( x \) to the system of congruences:
\[
\begin{align*}
\begin{cases}
  x \equiv \alpha & \pmod{a} \\
  x \equiv \beta & \pmod{b}
\end{cases}
\end{align*}
\]
Any two solutions are congruent modulo \( ab \).

**Proof**
Write \( sa + tb = 1 \), set \( x_1 = tb = 1 - sa \)
Then \( x_1 \equiv 1 \pmod{a} \) and \( x_1 \equiv 0 \pmod{b} \)
Set \( x_2 = sa = 1 - tb \).
Then \( x_2 \equiv 0 \pmod{a} \) and \( x_2 \equiv 1 \pmod{b} \)
A solution is
\[ x = \alpha x_1 + \beta x_2 \]
for, modulo \( a \):
\[ x \equiv \alpha x_1 + \beta x_2 \equiv \alpha \cdot 1 + \beta \cdot 0 \equiv \alpha \pmod{a} \]
modulo \( b \):
\[ x \equiv \alpha x_1 + \beta x_2 \equiv \alpha \cdot 0 + \beta \cdot 1 \equiv \beta \pmod{b} \]

Let \( x \) and \( x' \) be two solutions. 
Then 
\[ x \equiv x \equiv x' \pmod{a} \]
\[ x \equiv x' \pmod{b} \]
so \( a \mid (x-x') \) and \( b \mid (x-x') \) by lemma above, \( ab \mid x-x' \)
So \( x \equiv x' \pmod{ab} \)
\[ \square \]