CHAPTER 3: CONGRUENCES

§3.1 DEFINITIONS

IF a, b \in \mathbb{Z} we say \( a \equiv b \pmod{n} \) IF \( n \mid (a-b) \).

"a is congruent to b modulo n."

Clearly an equivalence relation: \( a \equiv a \pmod{n} \),

\( a \equiv b \pmod{n} \iff b \equiv a \pmod{n}, \) AND \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \)

\( \implies a \equiv c \pmod{n} \).

By a "complete set of residues mod n" we mean a
Set of representatives of each equivalence class
mod n, so for example \( 0, 1, 2, \ldots, n-1 \).

If \( a \equiv a' \pmod{n} \) and \( b \equiv b' \pmod{n} \) then it is easy
To verify \( a \pm b \equiv a' \pm b' \pmod{n} \) and \( ab \equiv a'b' \pmod{n} \).

So if \( f(x) \) is a polynomial with integer coefficients
\( f(a) \equiv f(a') \pmod{n} \).

If \( kc \equiv kc' \pmod{n} \) for some \( k \in \mathbb{N} \) with
\( (k,n) = 1 \) then \( c \equiv c' \pmod{n} \). Why? Two reasons
1) \( n \mid k(c-c') \) but \( (n,k) = 1 \) so \( n \nmid (c-c') \)
2) \( kx+ny=1 \) for some \( x, y \in \mathbb{Z} \) \( \iff \) \( kx \equiv 1 \pmod{n} \) for
Some \( x \in \mathbb{Z} \),

And so we can say \( k \) is "invertible"
Mod n IFF \( (k,n)=1 \), and we can call \( x \equiv k^{-1} \pmod{n} \).

So \( kc \equiv kc' \pmod{n} \) \( \iff \) \( k'kc \equiv k'kc' \pmod{n} \) \( \iff \) \( c \equiv c' \pmod{n} \).

Also \( k' \) is unique \( \pmod{n} \) since IF \( ak \equiv 1 \pmod{n} \) and \( bk \equiv 1 \pmod{n} \),

THEN \( akb \equiv a \equiv b \pmod{n} \).
IF \( a_1, a_2, \ldots, a_n \) is a complete set of residues modulo \( n \) and \( (k, n) = 1 \), then so is \( ka_1, ka_2, \ldots, ka_n \) (why?)

Also if \( k \in \mathbb{Z} \) with \( ka \equiv ka' \pmod{n} \), more generally
\[
a \equiv a' \pmod{(n, k)}, \quad \text{since} \quad n \mid k(a - a') \Rightarrow \frac{n}{(k, n)} \mid \frac{k}{(k, n)}(a - a')
\]
and \( \left( \frac{n}{(k, n)} \right) k = 1 \).

§ 3.2 CHINESE REMAINDER THEOREM

Sun Tzu's Remainder Theorem? (5th century).

Anyway...

**Claim:** Let \( a, n \in \mathbb{N} \) and \( b \in \mathbb{Z} \), then
\[
ax \equiv b \pmod{n}
\]
has a solution for \( x \in \mathbb{Z} \) \iff \( (a, n) \mid b \).

**Proof:** The condition is necessary since \( (a, n) \mid (ax - b) \) and \( (a, n) \mid a \) so \( (a, n) \mid b \).

For sufficiency, let \( d = (a, n) \) and let \( d \mid b \).

Denote \( a = a'd \), \( n = n'd \) and \( b = b'd \). If \( a'x \equiv b' \pmod{n'} \)
for some \( x \in \mathbb{Z} \) we are done since \( n' \mid a'x - b' \)
\[
\Rightarrow n' \mid (ax - b). \quad \text{So solve} \quad a'x \equiv b' \pmod{n'} \Rightarrow (a')^{-1}a'x \equiv (a')^{-1}b' \pmod{n'}
\]
so \( k \equiv (a')^{-1}b \pmod{n'} \) works and is a unique solution \( \pmod{n'} \). \( \square \)
Remark: If $x_0$ is the unique solution $(\mod n)$, then $x = x_0 + mn'$ is a solution $(\mod n)$ and we see there are $\frac{n}{n'}$ of these distinct solutions when a solution exists.

Every nonzero element $(\mod p)$ is invertible so the residues $0, 1, \ldots, p-1$ under modular arithmetic make a field, which we denote $\mathbb{Z}_p^*$. Similarly, the residues $0, 1, \ldots, n-1$ under arithmetic $(\mod n)$ make a ring: $\mathbb{Z}_n$.

Chinese Remainder Theorem

Let $n_1, n_2, \ldots, n_k \in \mathbb{N}$ with $(n_i, n_j) = 1$ for $i \neq j$ then for any $c_1, \ldots, c_k \in \mathbb{Z}$ there exists exactly one $x \in \mathbb{Z}$ which is a simultaneous solution to $x \equiv c_i \pmod{n_i}$ for all $i = 1, \ldots, k$ and the solution is unique mod $n_1n_2\ldots n_k$.

Proof: Let $N = n_1n_2\ldots n_k$ and $m_i = \frac{N}{n_i}$ for $i = 1, \ldots, k$. Then $(n_i, m_i) = 1$ for all $i$. So $m_ix_j \equiv c_j \pmod{n_j}$ has a unique solution for $x_j \pmod{n_j}$. Then $m_1x_1 + m_2x_2 + \ldots + m_kx_k \equiv c \pmod{N}$. This is our $x$.

Solution is unique since if $y$ is another solution then $n_i | (x - y)$ for all $n_i$ and $n_i$ are coprime.