Chapter 4. Fundamentals of Congruences

§ 4.1. Basic Properties of Congruences

Def. If \( \equiv 0 \), we say that \( a \equiv b \pmod{2} \)
if provided that \( \frac{a-b}{2} \) is an integer (or \( 2 \mid a-b \)).

Ex. 1  \( 7 \equiv 3 \pmod{4} \)
\( 17 \equiv 12 \pmod{5} \)
\( 7 \equiv 3 \pmod{8} \)
\( 100 \equiv -40 \pmod{20} \)
\( 14 \equiv -1 \pmod{15} \)

Ex. 2 If \( a \equiv b \), then for any \( 2 \), \( a \equiv b \pmod{2} \).
But \( a \equiv b \pmod{2} \) does not necessarily imply that \( a = b \).

Thm. 4.1 If \( a, b, c, \Theta, \Omega \) are integers (\( \equiv 0 \)), then
\( a \equiv a \pmod{2} \) — “reflective”
\( a \equiv b \pmod{2} \iff b \equiv a \pmod{2} \) — “symmetric”
If \( a \equiv b \pmod{2} \), \( b \equiv c \pmod{2} \), then
\( a \equiv c \pmod{2} \) — “transitive”

Proof is easy (fill in by yourself)
**Thm 4.2.** Suppose \( a \equiv a' \pmod{2} \), \( b \equiv b' \pmod{2} \)
then \( a \pm b \equiv a' \pm b' \pmod{2} \)
\( a \cdot b \equiv a' \cdot b' \pmod{2} \)

**Ex 3.** \( 19 \equiv 11 \pmod{4} \) and \( 6 \equiv 2 \pmod{4} \)

So \( 25 \equiv 13 \pmod{4} \) (add)
\( 13 \equiv 9 \pmod{4} \) (subtract)
\( 9 \cdot 14 \equiv 22 \pmod{4} \) (multiply)

However, division is not always OK.

**Ex. 4.** \( 15 \equiv 5 \pmod{10} \)
but \( 3 \not\equiv 1 \pmod{10} \)

**Thm 4.3.** (Cancellation law) If \( a \cdot b \equiv a' \cdot b' \pmod{2} \)
and \( (b, 2) = 1 \), then \( a \equiv a' \pmod{2} \)

**Ex. 5.** \( 6 \equiv 2 \pmod{2} \) and \( \gcd(3, 2) = 1 \),

So \( 2 \equiv 4 \pmod{2} \) by Thm 4.3.

but we cannot conclude that \( 3 \equiv 6 \pmod{2} \) (why?)
§ 4.2 Residue Systems

Def: If h, j integers and \( h \equiv j \pmod{m} \) then we say
j is a residue of h modulo m.

Def: The set of integers \( \{ r_0, r_1, \ldots, r_s \} \) is called a
complete residue system modulo m if
(i) \( r_i \not\equiv r_j \pmod{m} \) for any \( i \neq j \),
(ii) for every integer \( n \) there corresponds an \( r_i \) such that
\( n \equiv r_i \pmod{m} \).

Thm 4.4. If \( \{ r_0, r_1, \ldots, r_s \} \) is a complete residue system modulo m, then \( s = m \).

Corl. \( \{ 0, 1, 2, \ldots, m-1 \} \) is a complete residue system mod m.

Ex: \( \{ 0, 1, 2, 3 \} \), \( \{ 1, 3, 2, 8 \} \), \( \{ -1, -2, 0, 1 \} \)
\( \{ 10, 11, 12, 13 \} \) are all complete residue system mod 4.

Ex. Find an integer \( n \) that satisfies the congruence
\[ 325n \equiv 11 \pmod{3} \]
Since \( 325 \equiv 1 \pmod{3} \) \( 11 \equiv 2 \pmod{3} \)
so \( n \equiv 2 \pmod{3} \).
Def. The set of integers \( \{ r_1, r_2, \ldots, r_s \} \) is called a reduced residue system modulo \( m \) if

(i) \( \gcd (r_i, m) = 1 \) for each \( r_i \);

(ii) \( r_i \not\equiv r_j \pmod{m} \) whenever \( i \neq j \);

(iii) for each integer \( n \) relatively prime to \( m \) there corresponds an \( r_i \) such that \( n \equiv r_i \pmod{m} \).

Ex. \( \{ 0, 1, 2, 3, 4, 5 \} \) is a complete residue system modulo 6.
\( \{ 1, 5 \} \) is a reduced residue system modulo 6.

Ex. \( p \) is a prime; then \( \{ 0, 1, 2, \ldots, p-1 \} \) is a complete residue system modulo \( p \). The only element in this set not coprime to \( p \) is 0; hence \( \{ 1, 2, \ldots, p-1 \} \) is a reduced residue system modulo \( p \).

Def. The function \( \varphi(m) \) (called Euler's \( \varphi \)-function) shall denote the number of positive integers less than or equal to \( m \) that are relatively prime to \( m \).

Thm 4.5. If \( \{ r_1, \ldots, r_s \} \) form a reduced residue system modulo \( m \), then \( S = \varphi(m) \).
Ex. \( m = 4, \ \{1, 3\} \quad \varphi(4) = 2 \)

\( m = 5, \ \{1, 2, 3, 4\} \quad \varphi(5) = 4 \)

\( m = 6, \ \{1, 5\} \quad \varphi(6) = 2 \)

\( m = 8, \ \{1, 3, 5, 7\} \quad \varphi(8) = 4 \)

\( m = 9, \ \{1, 2, 4, 5, 7, 8\} \quad \varphi(9) = 6 \)

\( m = 10, \ \{1, 3, 7, 9\} \quad \varphi(10) = 4 \)

\( m = 11, \ \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \quad \varphi(11) = 10 \)

Do you see any obvious pattern for \( \varphi(m) \)?

We will study the exact formula for \( \varphi(m) \) in Chap 6.

\[ \text{Ex.} \]

Find integers such that

\[ 7x \equiv 6 \pmod{5} \quad \cdots \ (\times) \]

Since \( 7 \equiv 2 \pmod{5} \) and \( 6 \equiv 1 \pmod{5} \),

we may instead write \((\times)\) as

\[ 2x \equiv 1 \pmod{5} \quad \cdots \ (\ast\ast) \]

Now since \( 2 \times 3 \equiv 1 \pmod{5} \),

we multiply by 3 (which sort of plays the role of \( \frac{1}{2} \)

in the modulo 5 world) on both sides of \((\ast\ast)\)

\[ 6x \equiv 3 \pmod{5} \]

Hence \( x \equiv 3 \pmod{5} \).