Introduction to Congruences

Karl Friedrich Gauss developed congruences.

Definition: Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. We say that

a is congruent to b modulo m

if $m \mid (a-b)$.

If a is congruent to b modulo m, then we write

$$\boxed{a \equiv b \pmod{m}}$$

If $m \nmid (a-b)$, then we write

$$a \not\equiv b \pmod{m}$$

and we say that a is incongruent modulo m.

m = modulus of the congruence.

ex:

ex: Clocks work modulo 12 (or 24) for hours and modulo 60 for minutes and seconds.

ex: Calendars work modulo 7 for days of a week and modulo 12 for months.

ex: Odometers usually work modulo 1,000,000.

There is a relationship between congruences and equalities.

<u>Theorem 4.1:</u> Let $a, b \in \mathbb{Z}$. Then,

$$a \equiv b \pmod{m} \iff \exists\, k \in \mathbb{Z} \text{ s.t. } a = b + km$$

Proof: $a \equiv b \pmod{m} \iff m \mid (a-b)$

$\iff a - b = km$ for some $k \in \mathbb{Z}$

$\iff \exists\, k \in \mathbb{Z}$ s.t. $a = b + km$

Next, we show that congruence is an equivalence relation on $\mathbb{Z}$.

<u>Theorem 4.2:</u> Let $m \in \mathbb{Z}^+$. Then

(i) $a \equiv a \pmod{m}$ $\forall\, a \in \mathbb{Z}$ (Reflexivity)

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(Symmetry)

(iii) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$
$\Rightarrow a \equiv c \pmod{m}$

Proof: (i) $a - a = 0$ and $m \mid 0$, so $m \mid (a-a)$ for any $a \in \mathbb{Z}$.

$\therefore a \equiv a \pmod{m} \quad \forall a \in \mathbb{Z}$.

(ii) $a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$
$\Rightarrow a - b = mk$ for some $k \in \mathbb{Z}$.
$\Rightarrow b - a = m(-k)$
$\Rightarrow m \mid (b-a)$
$\Rightarrow b \equiv a \pmod{m}$

(iii) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$

$\Rightarrow m \mid (a-b)$ and $m \mid (b-c)$

$\Rightarrow m \mid ((a-b)+(b-c))$

$\Rightarrow m \mid (a-c)$

$\Rightarrow a \equiv c \pmod{m}$

An equivalence relation gives rise to equivalence classes. Let's look at an example.

ex: Find the equivalence classes of congruence modulo 3.

Let us find the equivalence classes of several elements.

$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\}$$
$$= \{x \in \mathbb{Z} : 3 \mid (x-1)\}$$
$$= \{x \in \mathbb{Z} : x - 1 = 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{1 + 3k : k \in \mathbb{Z}\}$$
$$= \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

Similarly,

$$[2] = \{\ldots -4, -1, 2, 5, 8, \ldots\}$$
$$[3] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[4] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$= [1]$$
$$[5] = [2]$$
$$[6] = [3] \text{ etc.}$$

Thus, $\ldots = [-3] = [0] = [3] = [6] = \ldots$

$$\cdots = [-2] = [1] = [4] = [7] = \cdots$$

$$\cdots = [-1] = [2] = [5] = [8] = \cdots$$

Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

By the division algorithm,

$$a = bm + r \text{ with } 0 \leq r \leq m-1.$$

r is called the least nonnegative residue of a modulo m.

We also say that

r is the result of reducing a modulo m.

Another notation commonly used in computer science is

$$a \bmod m = r$$

to denote the least nonnegative residue of a modulo m.

<u>Theorem 4.3:</u> Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then,

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Proof: Suppose $a \equiv b \pmod{m}$.

Then, $m \mid (a-b)$.

Let $r_1 = a \bmod m$ and $r_2 = b \bmod m$.

Then, $a = mq_1 + r_1$ and $b = mq_2 + r_2$

for some $q_1, q_2 \in \mathbb{Z}$ with $0 \le r_1, r_2 \le m-1$

Then $a - b - m(q_1 - q_2) = r_1 - r_2$

Then $m \mid (r_1 - r_2)$ $\left(\because m \mid (a-b) \text{ and } m \mid m(q_1 - q_2)\right)$

Since $0 \le r_1, r_2 \le m-1$, we get that

$$-(m-1) \le r_1 - r_2 \le m-1.$$

$\therefore$ $r_1 - r_2 = 0$ $\therefore$ $r_1 = r_2$

$\therefore$ $a \bmod m = b \bmod m$.

Next, suppose $a \bmod m = b \bmod m$.

Let $r_1 = a \bmod m$ and $r_2 = b \bmod m$.

Then, $a = mq_1 + r_1$ and $b = mq_2 + r_2$

$$\therefore a - b = m(q_1 - q_2) + \underbrace{r_1 - r_2}_{=0}$$

$\therefore m \mid (a-b)$

$\therefore a \equiv b \pmod{m}$.

By the division algorithm, we know that, for any $a, m \in \mathbb{Z}$ with $m > 0$,

$$a = mq + r \quad ; \quad 0 \leq r < m.$$

An equivalent statement is

$$a \equiv r \pmod{m} \text{ for some } 0 \leq r < m.$$

<u>Conclusion</u>: Every integer is congruent modulo m to one of $0, 1, 2, \ldots, m-1$.

<u>ex</u>: 12 is congruent modulo 5 to 2 because

$$12 \equiv 2 \pmod{5}$$

As we've seen before, equivalent ways to say this are

* 12 is congruent to 2 modulo 5
* 12 and 2 are congruent modulo 5.

<u>ex</u>: -7 is congruent to 2 modulo 3 because

$$-7 \equiv 2 \pmod{3}$$

(Note that $-7 = 3(-3) + 2$

<u>Definition</u>: A complete system of residues modulo m is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.

ex: $\{0, 1, 2, 3\}$ is a complete system of residues modulo 4.

Another such system is $\{1, 2, 3, 4\}$.
Another one is $\{8, 9, 10, 11\}$.
Another one is $\{0, 1, 10, 43\}$.
Another one is $\{-1, 0, 1, 2\}$.

ex: Let m be odd. Then

$$\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots \frac{m-3}{2}, \frac{m-1}{2}\right\}$$

is a complete system of residues modulo m.

Modular Arithmetic

Congruences, in a sense, behave similar to equalities.

Theorem 4.4: Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$. Suppose $a \equiv b \pmod{m}$. Then,

(i) $a + c \equiv b + c \pmod{m}$
(ii) $a - c \equiv b - c \pmod{m}$
(iii) $ac \equiv bc \pmod{m}$

Proof: Exercise

ex: $8 \equiv 3 \pmod 5$

How about division?

Observe that $14 \equiv 8 \pmod 6$ but

$$\frac{14}{2} \not\equiv \frac{8}{2} \pmod 6.$$

On the other hand,

$$18 \equiv 12 \pmod 3$$

and

$$\frac{18}{2} \equiv \frac{12}{2} \pmod 3.$$

When can we divide?

<u>Theorem 4.5</u>: Let $a, b, c, m \in \mathbb{Z}$ and $m > 0$. Let $d = \gcd(c, m)$. Then,

$$ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod{\tfrac{m}{d}}$$

Proof: $ac \equiv bc \pmod m \Rightarrow m \mid (ac - bc)$

$\Rightarrow ac - bc = mk$ for some $k \in \mathbb{Z}$.

$\Rightarrow c(a-b) = mk$

$\Rightarrow \frac{c}{d}(a-b) = \left(\frac{m}{d}\right)k$

$$\Rightarrow \left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right)(a-b)$$

Since $\gcd\left(\frac{c}{d}, \frac{m}{d}\right) = 1$, by Lemma 3.4, it follows that

$$\left(\frac{m}{d}\right) \mid (a-b)$$

$$\Rightarrow \quad a \equiv b \pmod{\frac{m}{d}}$$

<u>Corollary 4.5.1:</u> Let $a, b, c, m \in \mathbb{Z}$, $m > 0$ and $\gcd(m, c) = 1$. Then

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

Proof: Easily follows from the theorem since $d = 1$.

<u>ex</u>: $4 \times 8 \equiv 4 \times 2 \pmod{3}$

Since $\gcd(4,3) = 1$, we get

$$8 \equiv 2 \pmod{3}$$

<u>ex</u>: $3x \equiv 3y \pmod{5} \Rightarrow x \equiv y \pmod{5}$

$(\because \gcd(3,5) = 1)$

ex: $5x \equiv 10 \pmod{2} \Rightarrow x \equiv 2 \pmod{2}$

Theorem 4.6: Let $a, b, c, d, m \in \mathbb{Z}$ and $m > 0$.

Suppose $a \equiv b \pmod{m}$ and
$c \equiv d \pmod{m}$.

Then,

(i) $a + c \equiv b + d \pmod{m}$

(ii) $a - c \equiv b - d \pmod{m}$

(iii) $ac \equiv bd \pmod{m}$

Proof: Exercise

Lemma 4.1: Let $S = \{r_1, r_2, \ldots, r_m\}$ be a set of m incongruent integers modulo m (i.e., $r_i \not\equiv r_j \pmod{m}$ for all $i \neq j$). Then, this set is a complete system of residues modulo m.

Proof: Suppose S is not a complete system of residues modulo m.
Then, $\exists\, a \in \mathbb{Z}$ such that, for all i,

$$a \not\equiv r_i \pmod{m}. \quad \text{— (1)}$$

If $a \equiv mq + r$ with $0 \leq r \leq m-1$ (by division algorithm), then

$$a \equiv r \pmod{m}. \quad \text{— (2)}$$

from ① and ②, it follows that

$$r_i \not\equiv r \pmod{m} \text{ for all } i.$$

$\therefore$ the number of remainders of r_i's when divided by m is less than m. Therefore, not all r_i's are incongruent, i.e.,

$$r_i \equiv r_j \pmod{m}$$

for some i, j, a contradition because S is a set of incongruent integers modulo m.
Hence S is a complete system of residues modulo m.

<u>Theorem 4.7</u>: Suppose $r_1, r_2, \ldots, r_m$ is a complete system of residues modulo m, and $a \in \mathbb{Z}^+$ is such that $\gcd(a,m)=1$. Then,

$$ar_1+b,\ ar_2+b,\ \ldots,\ ar_m+b$$

is a complete system of residues modulo m.

Proof: Exercise

<u>Theorem 4.8</u>: Let $a, b, k, m \in \mathbb{Z}$ and $k, m > 0$. Then,

$$a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$$

Proof: Exercise.

ex: $5 \equiv 2 \pmod 3$, so $5^4 \equiv 2^4 \pmod 3$.

<u>Theorem 4.9</u>: Let a and b be integers and let $m_1, m_2, \dots, m_k$ be positive integers.

Suppose

$$a \equiv b \pmod{m_1}$$
$$a \equiv b \pmod{m_2}$$
$$\vdots$$
$$a \equiv b \pmod{m_k}$$

$14 \equiv 2 \pmod 2$

$14 \equiv 2 \pmod 3$

$\therefore 14 \equiv 2 \pmod 6$

Then, $a \equiv b \pmod m$ where

$$m = \operatorname{lcm}(m_1, m_2, \dots, m_k).$$

Proof: Exercise

<u>Corollary 4.9.1</u>: Let $a, b \in \mathbb{Z}$ and $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$.

Suppose $\gcd(m_i, m_j) = 1 \ \forall\, i \neq j$ and that

$$a \equiv b \pmod{m_i} \quad \forall\, i.$$

Then, $a \equiv b \pmod{m_1 m_2 \cdots m_k}$.

Fast Modular Exponentiation

How can we find, for example 2^{644} modulo 645?

It is not easy to find 2^{644}.
We wish to use a different method.
Let's learn it.

Step 1: Write 644 in base 2 and then write it in powers of 2.

$$644 = (1010000100)_2$$
$$= 2^9 + 2^7 + 2^2 = 512 + 128 + 4$$

Step 2: Compute the least positive residues of

$2^1, 2^2, 2^4, 2^8, 2^{16}, \ldots, 2^{512}$ modulo 645.

$2 \equiv 2 \pmod{645}$

$2^2 \equiv 4 \pmod{645}$

$2^4 \equiv 16 \pmod{645}$

$2^8 \equiv 256 \pmod{645}$

$2^{16} \equiv 256^2 \equiv 391 \pmod{645}$

$2^{32} \equiv 391^2 \equiv 16 \pmod{645}$

$2^{64} \equiv 16^2 \equiv 256 \pmod{645}$

$$2^{128} \equiv 256^2 \equiv 391 \pmod{645}$$

$$2^{256} \equiv 16 \pmod{645}$$

$$2^{512} \equiv 256 \pmod{645}$$

Step 3: Now, $2^{644} = 2^{512+128+4}$

$$= 2^{512} \cdot 2^{128} \cdot 2^{4}$$

$$\equiv 256 \cdot 391 \cdot 16 \pmod{645}$$

$$\equiv 1{,}601{,}356 \pmod{645}$$

$$\equiv 1 \pmod{645}$$

This example can be generalized as follows.

"To find b^N modulo m, where $b, N, m \in \mathbb{Z}^+$, first write

$$N = (a_k a_{k-1} \cdots a_1 a_0)_b,$$

find the least residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, and finally multiply the least positive residues modulo m of b^{2^j} for those j with $a_j = 1$, reducing modulo m after each multiplication.