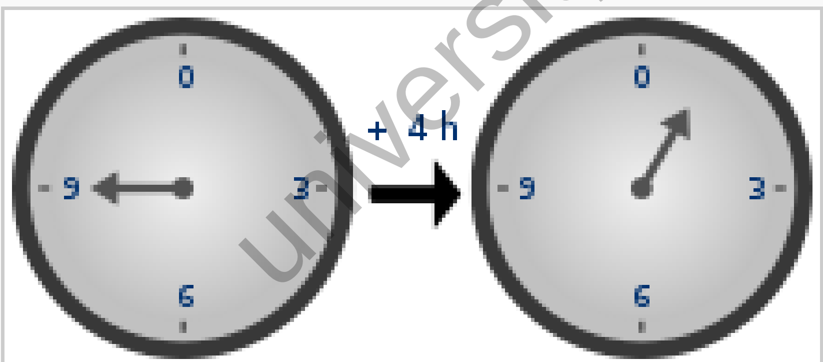
Modular Arithmetic & Chinese Remainder Theorem

Modular Arthmetic

- In mathematics, **modular arithmetic** (sometimes called **clock arithmetic**) is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the **modulus**.



Time-keeping on this clock uses arithmetic modulo 12.

Modular Arthmetic

- Modular arithmetic can be handled mathematically by introducing a congruence relation on the integers that is compatible with the operations of the ring of integers: addition, subtraction, and multiplication. For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n*, written:

$$a \equiv b \pmod{n},$$

- if their difference $a - b$ is an integer multiple of *n* (or *n* divides $a - b$). The number *n* is called the **modulus** of the congruence.

- The properties that make this relation a congruence relation (respecting addition, subtraction, and multiplication) are the follow $a_1 \equiv b_1 \pmod{n}$
- If $a_2 \equiv b_2 \pmod{n},$
- And
  - $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
- then:
  - $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$

- It should be noted that the above two properties would still hold if the theory were expanded to include all real numbers, that is if were not necessarily all integers. The next property, however, would fail if these variables were
  - $a_1 a_2 \equiv b_1 b_2 \pmod{n}.$

Chinese Theorem

- The **Chinese remainder theorem** is a result about congruences in number theory and its generalizations in abstract algebra. It was first published in the 3rd to 5th centuries by Chinese mathematician Sun Tzu.
- In its basic form, the Chinese remainder theorem will determine a number *n* that when divided by some given divisors leaves given remainders.
- For example, what is the lowest number *n* that when divided by 3 leaves a remainder of 2, when divided by 5 leaves a remainder of 3, and when divided by 7 leaves a remainder of 2?
- A common introductory example is a woman who tells a policeman that she lost her basket of eggs, and that if she makes three portions at a time out of it, she was left with 2, if she makes five portions at a time out of it, she was left with 3, and if she makes seven portions at a time out of it, she was left with 2.
- She then asks the policeman what is the minimum number of eggs she must have had. The answer to both problems is 23.

- Suppose n_1, n_2, …, n_k are positive integers that are pairwise coprime. Then, for any given sequence of integers a_1,a_2, …, a_k, there exists an integer x solving the following system of simultaneous congruences.

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions x of this system are congruent modulo the product, $N = n_1 n_2 \ldots n_k$.

Hence $x \equiv y \pmod{n_i}$ for all $1 \le i \le k$, if and only if $x \equiv y \pmod{N}$.

Example

Sometimes, the simultaneous congruences can be solved even if the n_i's are not pairwise coprime. A solution x exists if and only if:

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)} \qquad \text{for all } i \text{ and } j$$

All solutions x are then congruent modulo the least common multiple of the n_i.

Brute Force Technique:-

For example, consider the problem of finding an integer x such that

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 4$$
$$x \equiv 1 \pmod 5$$

A brute-force approach converts these congruences into sets and writes the elements out to the product of 3×4×5 = 60 (the solutions modulo 60 for each congruence):

x ∈ {2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, ...}

x ∈ {3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, ...}

x ∈ {1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, ...}

To find an x that satisfies all three congruences, intersect the three sets to get:

x ∈ {11, ...}

Which can be expressed as

$$x \equiv 11 \pmod{60}$$

Theorem 31.27 (Chinese remainder theorem)
Let $n = n_1 n_2 \cdots n_k$, where the n_i are pairwise relatively prime. Consider the correspondence

$$a \leftrightarrow (a_1, a_2, \ldots, a_k) , \tag{31.23}$$

where $a \in \mathbf{Z}_n$, $a_i \in \mathbf{Z}_{n_i}$, and

$$a_i = a \bmod n_i$$

for $i = 1, 2, \ldots, k$. Then, mapping (31.23) is a one-to-one correspondence (bijection) between $\mathbf{Z}_n$ and the Cartesian product $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$. Operations performed on the elements of $\mathbf{Z}_n$ can be equivalently performed on the corresponding k-tuples by performing the operations independently in each coordinate position in the appropriate system. That is, if

$$\begin{aligned} a &\leftrightarrow (a_1, a_2, \ldots, a_k) , \\ b &\leftrightarrow (b_1, b_2, \ldots, b_k) , \end{aligned}$$

then

$$(a + b) \bmod n \leftrightarrow ((a_1 + b_1) \bmod n_1, \ldots, (a_k + b_k) \bmod n_k) , \tag{31.24}$$

$$(a - b) \bmod n \leftrightarrow ((a_1 - b_1) \bmod n_1, \ldots, (a_k - b_k) \bmod n_k) , \tag{31.25}$$

$$(ab) \bmod n \leftrightarrow (a_1 b_1 \bmod n_1, \ldots, a_k b_k \bmod n_k) . \tag{31.26}$$

Thank You !!!