Modular Arithmetic

2019. 3. 19

Definition

Let a, r, m $\in$ Z and m>0.
Then

a $\equiv$ r mod m

if m divides (a-r), i.e., m|(a-r).

Some properties

$a \equiv b \bmod n \Leftrightarrow b \equiv a \bmod n$

$a \equiv b \bmod n$ and $b \equiv c \bmod n \Rightarrow a = c$

$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

$(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$

$(a \times b) \bmod n = ((a \bmod n) \text{ X } (b \bmod n)) \bmod n$

We can prove them by definition of modulo arithmetic.

$$(a+b) \bmod n = (b+a) \bmod n$$
$$(a \times b) \bmod n = (b \times a) \bmod n$$
$$((a+b)+c) \bmod n = (a+(b+c)) \bmod n$$
$$((a \times b) \times c) \bmod n = (a \times (b \times c)) \bmod n$$
$$(a \times (b+c)) \bmod n = ((a \times b) + (a \times c)) \bmod n$$

Equivalence Classes

Ex, m=5

$-3 \equiv 2 \bmod 5$

$2 \equiv 2 \bmod 5$

$7 \equiv 2 \bmod 5$

$12 \equiv 2 \bmod 5$

-3, 2, 7, 12 have the same behavior, i.e., the same remainder.

Def: the set {..., -8, -3, 2, 7, 12, 17,...} forms an "equivalent class modulo 5."
All members of the class behave equivalently
under the rule of the arithmetic of modulo 5

All equivalence classes of modulo 5

Class A (remainder = 0) : {..., -10, -5, 0, 5, 10, 15,...}
Class B (remainder = 1) : {..., -9, -4, 1, 6, 11, 16,...}
Class C (remainder = 2) : {..., -8, -3, 2, 7, 12, 17,...}
Class D (remainder = 3) : {..., -7, -2, 3, 8, 13, 18,...}
Class E (remainder = 4) : {..., -6, -1, 4, 9, 14, 19,...}

What does it mean? All numbers in the same class are actually the same.

$13 \times 16 - 8 = 200 \equiv 0 \bmod 5$
$3 \times 1 - 13 = -10 \equiv 0 \bmod 5$
$-7 \times 6 - 3 = -45 \equiv 0 \bmod 5$

What it implies

$$
\begin{aligned}
3^8 \bmod 7 &= 3^2 \times 3^2 \times 3^2 \times 3^2 \\
&= 9 \times 9 \times 9 \times 9 \\
&= 2 \times 2 \times 2 \times 2 \\
&= 16 \\
&= 2 \bmod 7
\end{aligned}
$$

What it really implies?

Identities and inverse

Additive identity: $(Y + 0) \bmod n = Y \bmod n$

Multiplicative identity : $(Y \times 1) \bmod n = Y \bmod n$

Additive inverse: $Y + (-Y) = 0 \bmod n$

Multiplicative inverse : $Y \times Y^{-1} = 1 \bmod n$ (?)

Multiplicative inverse

$a \times a^{-1} = 1 \bmod n$

a^{-1} exists if a and n are relatively prime, i.e., gcd(a,n) =1

Ex, $1^{-1}=?$ $1 \times (\ ) = 1 \bmod 5$
$2^{-1}=?$ $2 \times (\ ) = 1 \bmod 5$
$3^{-1}=?$ $3 \times (\ ) = 1 \bmod 5$
$4^{-1}=?$ $4 \times (\ ) = 1 \bmod 5$
$5^{-1}=?$ $5 \times (\ ) = 1 \bmod 5$

Ex, $1^{-1}=?$ $1 \times (\ ) = 1 \bmod 6$
$2^{-1}=?$ $2 \times (\ ) = 1 \bmod 6$
$3^{-1}=?$ $3 \times (\ ) = 1 \bmod 6$
$4^{-1}=?$ $4 \times (\ ) = 1 \bmod 6$
$5^{-1}=?$ $5 \times (\ ) = 1 \bmod 6$
$6^{-1}=?$ $6 \times (\ ) = 1 \bmod 6$

How can we find the multiplicative inverse? By The Extended Euclidian Algorithm