BECOME A MEMBER

ON STEADY

The Bright Side of Mathematics

Algebra - Part 8

modulus calculation:

$13 - \underset{\substack{\uparrow \\ \text{modulus} \\ = m}}{12} = 1$

$24 - 2 \cdot 12 = 0$

$x \sim_m y \iff$ There is $q \in \mathbb{Z}$: $x - y = q \cdot m$

$x \equiv y \pmod{m}$

Integers modulo m: $\mathbb{Z}_m$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/m$, $\mathbb{Z}/\sim_m$

$$\mathbb{Z}_m := \{[0], [1], \dots, [m-1]\}, \qquad m \in \mathbb{N}$$

for example with $m = 12$: $[2] = \{2, 14, 26, 38, \dots, -10, -22, \dots\}$

define addition: $[k] + [\ell] := [k + \ell]$ well-defined

$[k] + [-k] = [0]$ identity

inverse

$\Rightarrow (\mathbb{Z}_m, +)$ abelian group of order m

Example: $(\mathbb{Z}_2, +)$: $[0] = \{0, 2, 4, \dots, -2, -4, \dots\}$

$[1] = \{1, 3, 5, 7, \dots, -1, -3, \dots\}$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$(\mathbb{Z}_6, +)$: $[0] = \{0, 6, 12, \dots, -6, -12, \dots\}$

$[1], [2], [3], [4], [5]$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]				
[2]	[2]	[3]	[4]			
[3]	[3]	[4]	[5]	[0]		
[4]	[4]	[5]	[0]	[1]	[2]	
[5]	[5]	[0]	[1]	[2]	[3]	[4]