Modular Subtraction

Introduction to Rings

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Video 2/3
Recorded: September 20, 2013

Modulus

We are familiar with the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$*.*

- The modulus operation gives us two operations on $\mathbb{Z}_n$:
  1. Addition $+_n$
  2. Multiplication $\times_n$
- What about other operations?
  1. Subtraction
  2. Division

Subtraction

- Subtraction in $\mathbb{Z}_n$ works like addition

$$x -_n y = x - y \mod n$$

A general definition of division in rings require some further ideas.

The Zero Element

- Note that $0 \in \mathbb{Z}_n$.
- What is a zero?

$$\forall x \in \mathbb{Z}_n, \quad x + 0 = 0 + x = x$$

- Zero is the neutral element with respect to addition.

The Zero Element

- Note that $0 \in \mathbb{Z}_n$.
- What is a zero?

$$\forall x \in \mathbb{Z}_n, \quad x + 0 = 0 + x = x$$

- Zero is the neutral element with respect to addition.

Additive Inverses

$$\forall x \in \mathbb{Z}_n, \exists y \in \mathbb{Z}_n, \quad x + y = 0$$

- we write $(-x)$ for y
- $(-x)$ is the additive inverse
- Subtraction is defined as

Definition

Subtraction in any ring is defined as

$$x - y = x + (-y)$$

Exercise

Exercise

Consider the following elements x in their respective rings. Find $-x$ for each value of x.

1. $x = 8 \in \mathbb{Z}_{26}$
2. $x = 7 \in \mathbb{Z}_{29}$
3. $x = 1 \in \mathbb{Z}_2$