# Modular addition

## Introduction to Rings

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Video 2/1
Recorded: September 19, 2013

# Modulus

*The modulus operator is a cornerstone for cryptography.*

- Integer division

$$m = n \cdot q + r, \quad r < q$$

- We get the remainder term $r$
- This is the modulus operator
  - $m \mod n = r$
- $r \in \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

*We will discuss the properties and operations on the set $\mathbb{Z}_n$.*

HØGSKOLEN I ÅLESUND
Aalesund University College

# Binary operations

- A binary operation on a set $S$ is a function

$$f : S \times S \to S$$

- For instance, addition $(x + y)$

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

- Addition works on many different sets,
  - Rational numbers $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$
  - Integers $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
  - Natural numbers $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

# Closed set

*We say that $\mathbb{Z}$ is closed under addition*

$$\forall x, y \in \mathbb{Z}, x + y \in \mathbb{Z}.$$

- What about $\mathbb{Z}_{26}$?
- $14, 15 \in \mathbb{Z}_{26}$ but $14 + 15 = 29 \notin \mathbb{Z}_{26}$
- $\mathbb{Z}_{26}$ is not closed under integer addition.
- $\mathbb{Q}$, $\mathbb{N}$, and $\mathbb{R}$ (like $\mathbb{Z}$) are closed under addition.

### Definition

A set $S$ is said to be closed under an operation $O$ if, for all $x, y \in S$, we have $xOy \in S$.

## Addition in $\mathbb{Z}_n$

- Addition is also defined in $\mathbb{Z}_n$

$$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \tag{1}$$
$$x +_n y = x + y \mod n \tag{2}$$

- For instance, generalised Cæsar's cipher is given by

$$e_k(x) = x +_{26} k \tag{3}$$

- $\mathbb{Z}_n$ is closed under $+_n$
  - we refer to $+_n$ as addition in $\mathbb{Z}_n$
  - we could even write $+$ for $+_n$

HØGSKOLEN I ÅLESUND
Aalesund University College