Modular multiplication and rings

Introduction to Rings

Prof Hans Georg Schaathun

Høgskolen i Ålesund

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

Binary operations

- Common binary operations on a set S:

$$\cdot, + : S \times S \to S$$

- For instance, addition

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

Definition

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

Multiplication modulo n

We can also have multiplication in $\mathbb{Z}_{26}$.

$$x \times_{26} y = xy \mod 26$$

- Z_{26} is closed under $\times_{26}$
- We can also have exponentiation

$$x^n = x \times_{26} x \times_{26} \ldots \times_{26} x, \quad (n \text{ times})$$

HØGSKOLEN I ÅLESUND
Aalesund University College

The Ring $\mathbb{Z}_{26}$

Addition $+_{26}$ and multiplication $\times_{26}$ in $\mathbb{Z}_{26}$ work largely as we are used to in $\mathbb{R}$.

- Commutative $x +_{26} y = y +_{26} x$ and $x \times_{26} y = y \times_{26} x$
- Associative $x +_{26} (y +_{26} z) = (y +_{26} x) +_{26} z$ and $x \times_{26} (y \times_{26} z) = (x \times_{26} y) \times_{26} z$
- Distributive $x \times_{26} (y +_{26} z) = (x \times_{26} y) +_{26} (x \times_{26} z)$

$\mathbb{Z}_{26}$ is an example of a ring, just like $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Q}$.
We will discuss the precise properties rings later.

Affine cipher

- We can use both addition and multiplication for the encryption function.
- Take a key $(k_1, k_2) \in \mathbb{Z}_{26}^2$
- Take a letter represented as $x \in \mathbb{Z}_{26}$, and encrypt

$$e_{k_1,k_2}(x) = k_1 \times_{26} x +_{26} k_2$$

- E.g. $(k_1, k_2) = (3, 1)$
- Plaintext: `hi`
  - `hi` $\mapsto (7, 8)$
    - $7 \mapsto 3 \times_{26} 7 +_{26} 1 = 22$
    - $8 \mapsto 3 \times_{26} 8 +_{26} 1 = 25$
  - $(22, 25) \mapsto$ `wz`
- Ciphertext: `wz`

Exercise

Exercise

Encrypt the message `new idea`*, using the affine cipher with each of the following keys:*

1. $(3, 1)$
2. $(9, 3)$
3. $(5, -5)$

Exercise

Encrypt the message `an idea`*, using the encryption function* $e_{k_1,k_2}(x) = k_1 \times_{26} x +_{26} k_2$*, using the key* $(k_1, k_2) = (2, 2)$*. Comment on the result.*