Multiplicative Inverses

Introduction to Rings

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Video 2/4 Recorded: September 20, 2013



Modulus

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

- The modulus operation gives us two operations on \mathbb{Z}_n :
 - **1** Addition $+_n$
 - 2 Multiplication \times_n
 - 3 Subtraction -n

Can we have division?



Multiplicative Identity

- We know that $1 \in \mathbb{Z}_n$.
- what is a one?
- Zero (0) is neutral with respect to addition
- One (1) is neutral with respect to multiplication

$$\forall x \in \mathbb{Z}_n, x \cdot 1 = x$$

Every ring has identity (1)



Multiplicative Identity

- We know that $1 \in \mathbb{Z}_n$.
- what is a one?
- Zero (0) is neutral with respect to addition
- One (1) is neutral with respect to multiplication

$$\forall x \in \mathbb{Z}_n, \ x \cdot 1 = x$$

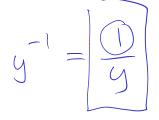
Every ring has identity (1)



Division of Real Numbers



$$\frac{\chi}{y} = \chi \cdot y$$



4/10

Integer Division

$$\frac{\chi}{y} = maybe not$$

$$\begin{array}{l}
\chi = 8 \\
y = 4
\end{array}$$

$$\frac{8}{4} = 2$$

Multiplicative inverse

Can we have division in \mathbb{Z}_{26} ?

Like subtraction, division is defined in terms of an inverse

$$x/y = x \times_{26} y^{-1}$$
, where $y \times_{26} y^{-1} = 1$

- Does every $x \in \mathbb{Z}_{26}$ have an inverse x^{-1} ?
- Clearly, some elements have an inverse
 - $3 \cdot 9 = 9 \cdot 3 = 27$
 - so $3 \times_{26} 9 = 9 \times_{26} 3 = 1$
 - and hence $3^{-1} = 9$ and $9^{-1} = 3$



Multiplicative inverse

Can we have division in \mathbb{Z}_{26} ?

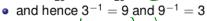
Like subtraction, division is defined in terms of an inverse

$$x/y = x \times_{26} y^{-1}$$
, where $y \times_{26} y^{-1} = 1$

- Does every $x \in \mathbb{Z}_{26}$ have an inverse x^{-1} ?
- Clearly, some elements have an inverse

•
$$3 \cdot 9 = 9 \cdot 3 = 27$$

• so
$$3 \times_{26} 9 = 9 \times_{26} 3 = 1$$





Problem

- Recall the affine cipher $e_{k_1,k_2}(x) = k_1 \times_{26} x + k_2$
- What happens with the key $(k_1, k_2) = (2, 2)$?
- Consider to letters a and n
- Encrypt

$$\widehat{n} \mapsto 13 \mapsto 2 \times_{26} 13 +_{26} 2 = 0 +_{2} \mapsto \widehat{c}$$
 (2)

- Decryption will not be unique
 - c could be either a or n



Zero divisors

We just encountered zero divisors

- Recall that for $x, y \in \mathbb{R}$ (or $x, y \in \mathbb{Z}$)
 - xy = 0 if and only if either x = 0 or y = 0
- Does this hold for $x, y \in \mathbb{Z}_{26}$?
- No, for x = 2 and y = 13, we have

$$2 \cdot 13 = 26 \quad \Rightarrow \quad 2 \otimes 13 = 0$$

2 and 13 are called zero divisors in Z₂₆



Zero divisors

We just encountered zero divisors

- Recall that for $x, y \in \mathbb{R}$ (or $x, y \in \mathbb{Z}$)
 - xy = 0 if and only if either x = 0 or y = 0
- Does this hold for $x, y \in \mathbb{Z}_{26}$?
- No, for x = 2 and y = 13, we have

$$2 \cdot 13 = 26 \quad \Rightarrow \quad 2 \otimes 13 = 0$$

2 and 13 are called zero divisors in Z₂₆

