# 50.020 Security
# Lecture 12 - Modular Arithmetics I

# This lecture



- This lecture: math!
- In particular:
  - Why we need groups, rings, fields in cryptography
  - Introduction to groups, rings, fields
  - References (on abstract algebra): `https://math.berkeley.edu/~apaulin/AbstractAlgebra.pdf`, `http://www-users.math.umn.edu/~garrett/m/algebra/notes/Whole.pdf`

# Where will we need that?



- We discussed S-Boxes in AES
  - How to choose the parameters
- We discussed MixColumn in AES
  - What is really happening in there
- We discussed XOR or $+$ for OTP
  - Why are they the same?
- We will discuss RSA in detail soon
- All these things rely on modular arithmetics

# Why do we need modular arithmetics?



- Because we are computing in finite resources
- int is 32 bit, long is 64 bit, ...
- Remember Caesar's cipher: only 26 symbols
  - What is Z shifted to the right by 3?
- How to solve? Limit space with a modulus
  - Will this change any of our arithmetic rules?
- For all this, we need *Galois (Extension) Fields* GF($p^n$)
  - But to explain those, we need groups, rings, fields

# Modular arithmetics



- Everyone knows the *mod* operation

```
>>> 8 % 5
3
```

- 3 is the *remainder* of 8 *modulus* 5
- Mathematical notation:
  - $8 \equiv 3 \mod 5$

More general for $\mathbb{Z}$, i.e. all integers={. . . ,-2,-1,0,1,2,. . . }

- $a \equiv r \mod m$, with $a, r, m \in \mathbb{Z}$
- Is there more than one solution to this congruence? Infinitely many!
  - $-2 \equiv 3 \mod 5$
  - $-7 \equiv 3 \mod 5$
  - $13 \equiv 3 \mod 5$
  - . . .

# Sets, Groups, Rings, Fields,...



- By convention, we chose the remainder from $0 \leq r < m$
- We obtain a set of possible elements $\mathbb{S} = \{0, 1, 2, \ldots, m-1\}$
- While $\mathbb{Z}$ is infinite, $\mathbb{S}$ is finite
- There are many other ways to construct sets
- Together with operators, they form algebraic structures
- Algebraic structures are classified based on
  - Properties of the set
  - Properties of the operator(s)
- Possible structures are *groups*, *rings*, *fields*,...

# Groups

# Arithmetic groups

## Definition (Group)

A *group* consists of:

- A set of elements
- An operation $\star$ that combines two elements to a third
- The operation $\star$ must satisfy the following properties:
  - closure
  - associativity
  - identity
  - invertibility

# Closure

## Definition (Closure)

An operation $\star$ on members of set satisfies *closure*, iff for all possible inputs from the set, the result of the operation is within the set.

## Example ($\mathbb{Z}^+$ and $+$,-)

- Positive integers $\mathbb{Z}^+$ and $+$ has closure
- Positive integers $\mathbb{Z}^+$ and - does not have closure

# Associativity

## Definition (Associativity)

An operation $\star$ on members of a set satisfies *associativity*, iff in an expression containing two or more operators, the order of evaluation does not change the result.

## Example ($\mathbb{Z}$ and *,$+$)

- $\mathbb{Z}$ and * is associative
- $\mathbb{Z}$ and $+$ is associative

# Identity

50.020 Security Lecture 12 - Modular Arithmetics I

Modular arithmetics

Modular arithmetics in AES

## Definition (Identity)

An operation $\star$ on members of a set satisfies *identity*, iff the set contains an element "0", such that $0 \star a = a$, $\forall a \in$ set

## Example ($\mathbb{Z}$ and *,$+$)

- $\mathbb{Z}$ and *: element 1 is identity
- $\mathbb{Z}$ and $+$: element 0 is identity

# Invertibility



## Definition (Invertibility)

An operation $\star$ on members of a set $\mathbb{S}$ satisfies *invertibility*, iff $\mathbb{S}$ contains an inverse $y \in \mathbb{S}$ for each $x \in \mathbb{S}$ such that $x \star y = y \star x = i$ (with $i$ the identity element of the operation).

## Example ($\mathbb{Z}$ and *,+)

- $\mathbb{Z}$ and *: no inverse for most elements, e.g. 2 *?=1
- $\mathbb{Z}$ and $+$: -a is inverse element for a

# Invertibility



## Definition (Invertibility)

An operation $\star$ on members of a set $\mathbb{S}$ satisfies *invertibility*, iff $\mathbb{S}$ contains an inverse $y \in \mathbb{S}$ for each $x \in \mathbb{S}$ such that $x \star y = y \star x = i$ (with $i$ the identity element of the operation).

## Example ($\mathbb{Z}$ and *,$+$)

- $\mathbb{Z}$ and *: no inverse for most elements, e.g. 2 *?$=$1
- $\mathbb{Z}$ and $+$: -a is inverse element for a

- Do you have an example group with an operation $\star$ that provides closure, associativity, identity, invertibility?

# Example group $(\mathbb{Z},+)$



- Based on the previous examples, $(\mathbb{Z},+)$ is an *additive group*
- Closure: for any $a, b \in \mathbb{Z}$, $c = a + b$ will have $c \in \mathbb{Z}$
- Associativity: for any $a, b, c \in \mathbb{Z}$: $(a+b)+c = a+(b+c)$
- Identity: for any $a \in \mathbb{Z}$, 0 is the identity: $a + 0 = a$
- Invertibility: for any $a \in \mathbb{Z}$, $-a$ is the inverse: $a + (-a) = (-a) + a = 0$

# Quotient groups



- So far, we only considered infinite groups
- Finite groups are much more interesting. Why?
- *Quotient groups* map a larger group onto a smaller one while preserving the structure
- For now, lets assume this mapping is the modulo operation

## Example ($\mathbb{Z}/2\mathbb{Z}$)

- Group created by "applying mod 2"
- $\mathbb{Z}/2\mathbb{Z}$ has two elements: $\{0,1\}$.
- Operations possible on these elements:
  - addition mod 2 (same as XOR )
  - Multiplication mod 2 (same as AND)

# Order of finite groups and elements

- The order of a group G is $|G|$, the number of its elements
- The order of an element is defined as follows

**Definition (Order of elements)**

The order of an element $a$ of a group $(\mathbb{S}, \star)$ is the smallest positive integer $k$ such that
$a^k = a \star a \star a \ldots a \star a = 1$
With 1 being the identity element for $\star$

# Cyclic groups

- Generated from one element $g$ with invertible associative operation. $G = \{g^n | n \in \mathbb{Z}\}$
- $g$ has order $|G|$, it is also called a primitive element or generator
- $(\mathbb{Z}^+, +)$ is a cyclic group with generator 1.

# Rings

# Arithmetic rings



- Arithmetic rings are groups with a second operation $\times$
- This operation is often called "multiplication", but can be any operation
- Requirements for $\times$:
  - This second operation $\times$ is associative
  - $\times$ needs to satisfy closure
  - $\times$ has an identity element
  - $\times$ is *distributive* over $\star$

# Distributivity



## Definition (Distributivity)

Consider two binary associative operations $\star, \times$ on members of a set $\mathbb{S}$. $\times$ is *distributive* over $\star$ iff $\forall a, b, c \in \mathbb{S}$:
$a \times (b \star c) = a \times b \star a \times c$

## Example ($\mathbb{Z}$ and * and $+$)

- $\mathbb{Z}$ and $+$,*: * is distributive over $+$
- $\mathbb{Z}$ and *,$+$: $+$ is not distributive over *

# Distributivity



## Definition (Distributivity)

Consider two binary associative operations $\star, \times$ on members of a set $\mathbb{S}$. $\times$ is *distributive* over $\star$ iff $\forall a, b, c \in \mathbb{S}$:
$a \times (b \star c) = a \times b \star a \times c$

## Example ($\mathbb{Z}$ and * and $+$)

- $\mathbb{Z}$ and $+$,*: * is distributive over $+$
- $\mathbb{Z}$ and *,$+$: $+$ is not distributive over *

- So, do you know an example for a Ring?

# Example ring ($\mathbb{Z}$,+,*)

- Based on the previous examples, ($\mathbb{Z}$,+,*) is a *ring*
- We know that ($\mathbb{Z}$,+) is a group
- The additional operation *
  - Is associative (a*b)*c=a*(b*c)
  - * is closed over $\mathbb{Z}$
  - Has identity element 1
  - Is distributive over +: a*(b+c)=a*b+a*c

# Fields

# Fields



- A *field* is a ring with the following properties:
- All elements of the field form an additive group with the group operation $+$ and the neutral element 0.
- All elements of the field except 0 form a multiplicative group with the group operation $\times$ and the neutral element 1.
    - In particular: each nonzero element has a multiplicative inverse
- When the two group operations are mixed, the distributivity law holds, i.e., for all a, b, c $\in \mathbb{S}$: $a*(b + c) = (a*b) + (a*c)$.

# Finite Fields



- Also called Galois Field: GF(p)
- p is called the *characteristic* of the field

**Example (GF(p))**

- p is prime number
- operations $+$,*
- In GF(2) addition is XOR, multiplication is AND

# Extension fields



- An arithmetic structure that "contains several instances of a basic field"
- The basic field is also called a subfield of the extension field
- Example: $GF(p^n)$ with $GF(p)$ as subfield
- Field operations $\star$ and $\times$ can still be applied to elements of the extension field
- Commonly, a polynomial representation is used for the elements

# Polynomials

- We represent our elements of GF($p^n$) as coefficients of a polynomial of degree $n-1$
- The coefficients are each in GF(p)
- Example: GF($2^8$):
  $P(x)=a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$
- These "$x^n$" are placeholders, not the variable to be evaluated
- For multiplication (and division), "schoolbook" polynomial division can be used
  - But the result has to be *reduced* mod a fixed irreducable polynomial of degree $n$
- Addition and subtraction are simple XORs of the vectors/coefficients

# Example: $GF(2^2)$



- Subfield is $GF(2)=(\{0,1\},+,*)$
- Elements can be represented as 2 bit values, e.g. 01
- Additions are XOR within the respective subfield
  - 10+11 =01
- Multiplications are polynomial multiplications within the respective subfields
  - $=10*11 = x^2+x = 110 =$ which is of degree 2...
- Lets assume our reduction polynomial is $P(x)=x^2+x+1$
  - Reduction operation: $(x^2 + x) \bmod x^2+x+1 = 110$ - $111$
  - $= 110$ XOR $111 = 001$
- Still confused? More details are coming up (next lecture)

# GF($2^8$) in AES



- GF($2^8$) is used for the S-boxes and mixColumn in AES
- Particular irreducible polynomial is chosen, Rijndael's polynomial
  - $P(x)=x^8+x^4+x^3+x+1$
- S-Boxes are usually hard-coded, but can also be replaced by GF($2^8$) multiplication/division

# Byte Substitution



- In AES, byte substitution for $A_i$ (in $GF(2^8)$) requires the computation of the multiplicative inverse, and then an affine mapping.
- The multiplicative inverse can be computed on-the-fly using the extended euclidean algorithm
- We will discuss that algorithm in more detail in next lecture

# Conclusion

- Cryptographic operations rely on modular arithmetics
- They allow us to work on limited hardware
- We can still preserve some "hardness guarantees"
  - More on that later
- To construct Galois Fields, we need the characteristic to be a prime
- Extension fields need to have an irreducable polynomial instead
- More details next lecture