50.042 FCS Summer 2024
Lecture 9 – Modular Arithmetic I

Felix LOH
Singapore University of Technology and Design

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

With selected materials adapted from: *Understanding Cryptography: A Textbook for Students and Practitioners, by C. Paar and J. Pelzl*

Modular arithmetic: rationale

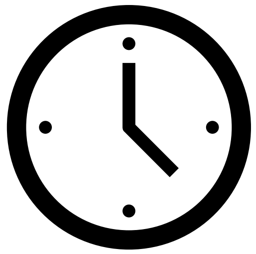
- We have already discussed a bit of modular arithmetic, back in Lectures 1 and 2
  - We saw how the XOR operation is really addition modulo 2
  - We will see that XOR is also addition in the Galois field $GF(2)$
- In this and the next lecture, we will go into modular arithmetic concepts in depth
- This is necessary for us to better understand the Byte Substitution layer (S-boxes) and MixColumn sublayer of AES; both of these rely on modular arithmetic
- We will also discuss the Diffie-Hellman key exchange and RSA cryptosystems soon, this requires an understanding of modular arithmetic concepts as well

Modular arithmetic: rationale

- Modular arithmetic falls under the area of *Number Theory*
- We need to understand modular arithmetic, because computing devices calculate with finite resources
  - Integer and float are 32-bit or 64-bit datatypes
  - Long is a 64-bit datatype
  - Operations with these datatypes can lead to overflow/underflow
- Back in Lecture 2, we saw that Caesar's cipher operates on a set of 26 alphabetical characters, and to encrypt, we shift the plaintext character by some constant value *k*
  - If we shift (add) the character 'z' by 3, we need to "constrain" or "limit" the shift operation to ensure that it operates within the set
  - This is an addition *modulo* 26 operation, as we saw in Lecture 2

Modular arithmetic (recap)

- Modular arithmetic is basically a way to perform arithmetic with a **finite** set of integers
- Example: Analog clocks
  - Keep adding 1 hour to the hours of the clock
  - 1 o'clock, 2 o'clock, 3 o'clock, …, 11 o'clock, 12 o'clock, 1 o'clock, …
  - We never leave the finite set of integers {1, 2, 3, …, 10, 11, 12}



Modulo operation (formal definition, recap)

- Let *a, r, m* ∈ ℤ (i.e. *a*, *r* and *m* are members of ℤ, the set of all integers), with $m > 0$

  We write *a ≡ r mod m*, if *m* divides *a – r*

  r is called the *remainder* and *m* is called the *modulus*

- Notes:
  - Strictly speaking, the remainder is **not unique,** because mathematically, it's **not** required that *0 ≤ r < m* (unlike Python)
  - So there are infinitely many values of *r* for any given *a* and *m*
  - E.g. 7 ≡ 7 *mod* 4, 7 ≡ 3 *mod* 4, 7 ≡ -1 *mod* 4, and so on
  - However, by convention, we choose *r* such that *0 ≤ r < m*, so in the above example, we pick 7 ≡ 3 *mod* 4

congruent

{0, 1, 2, 3}

{4, 5, 6, 7}

{8, 9, 10, 11}

mapped to the same number

7 mod 4 = 3

3 mod 4 = 3

-1 mod 4 = 3

Computation of the remainder (recap)

- It is always possible to express $a \in \mathbb{Z}$ in the form of $a = q \times m + r$, with $0 \leq r < m$
- Since $a - r = q \times m$, this means that m divides $a - r$, so we can write

  $a \equiv r \ mod \ m$
- E.g. Let $a = 42$, and $m = 9$. Then $42 = 4 \times 9 + 6$ and therefore,

  $42 \equiv 6 \ mod \ 9$

Algebraic structures and operations

- An *algebraic structure* is a set of elements, along with one or more operations which act on the elements of the set

- An *operation* (or *operator*) is a function which combines two input values (which are called operands) into a well-defined output value

Algebraic structures and related properties

- We will discuss the following properties related to algebraic structures:
  - Closure
  - Associativity
  - Identity
  - Invertibility
  - Commutativity and Distributivity
- We'll also discuss the following algebraic structures:
  - Groups
  - Rings
  - Fields
  - Finite fields (Galois fields)
  - Prime fields
  - Extension fields

Closure: definition

- An operation on elements of a set satisfies the **closure** property, if and only if for all possible input values (operands) from that set, the output value (result) of that operation is also an element of the set
- i.e. An operation ○ for a set S satisfies closure, if and only if

  $a \circ b = c \in S$ for all $a, b \in S$

$2 \quad + \quad 16 \quad 256 \quad 512 \quad 1024$

$2^1 + 2^4 + 2^8 \quad 2^9 + 2^{10}$

$2^1 \equiv 2 \bmod 7 \quad 2^4 \equiv 2 \bmod 7 \quad 2^9 \equiv 2^1 \cdot 2^8 \bmod 7 \quad 11 \bmod 7$

$\equiv 1 \bmod 7 \quad 4 \bmod 7$

$2^2 \equiv 4 \bmod 7 \quad 2^8 \equiv 4 \bmod 7 \quad 2^{10} \equiv 2 \bmod 7$

$$\begin{array}{r} 1024 \\ 512 \\ \hline 1536 \\ 256 \\ \hline 1792 \end{array}$$

- E.g.
  - The addition operator '+' for the set of all positive integers $\mathbb{Z}^+$ satisfies closure
  - The subtraction operator '–' for the set of all positive integers $\mathbb{Z}^+$ does **not** satisfy closure
  - The subtraction operator '–' for the set of all integers $\mathbb{Z}$ satisfies closure

Associativity: definition

- An operation on elements of a set satisfies the **associativity** property, if and only if in an expression containing multiple operations, the order of evaluation of the operations does **not** change the result of that expression
- i.e. An operation $\circ$ for a set S satisfies associativity, if and only if

  $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in S$
- E.g.
  - The addition operator '+' for the set of all integers $\mathbb{Z}$ satisfies associativity
  - The multiplication operator '$\cdot$' (or '$\times$') for the set of all integers $\mathbb{Z}$ satisfies associativity
  - The addition operator '+' for the set of all real numbers $\mathbb{R}$ satisfies associativity

Identity: definition

- An operation $\circ$ on elements of a set S satisfies the **identity** property, if and only if there is an identity element $i \in S$ (with respect to the operation $\circ$), such that

  $i \circ a = a \circ i = a$ for all $a \in S$

- E.g.
  - The addition operator '+' for the set of all integers $\mathbb{Z}$ satisfies the identity property, since $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$ (with additive identity element 0)
  - The multiplication operator '·' for the set of all integers $\mathbb{Z}$ satisfies the identity property, since $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$ (with multiplicative identity element 1)

Invertibility: definition

- An operation ○ on elements of a set S satisfies the **invertibility** property, if and only if for each element $a \in S$, the inverse $a^{-1} \in S$ also exists, such that

  $a \circ a^{-1} = a^{-1} \circ a = i$, where $i \in S$ is the identity element with respect to the operation ○

- E.g.
  - The addition operator '+' for $\mathbb{Z}$ satisfies the invertibility property, since the additive inverse of a is $-a$, with $a + (-a) = (-a) + a = 0$ for all $a \in \mathbb{Z}$ (with additive identity element 0)
  - The multiplication operator · for $\mathbb{Z}$ does **not** satisfy the invertibility property, since the multiplicative inverse does not exist for most elements of $\mathbb{Z}$

0^{-1} has no inverse.

Group: definition

- A group $G = (S, \circ)$ is a set of elements, S, together with an operation $\circ$ which combines two elements of S. A group **must** have the following four properties:

- The group is **closed**, i.e. $a \circ b = c \in S$ for all $a, b \in S$
- The group operation is **associative**, i.e. $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in S$
- There is an **identity** element $i \in S$ with respect to the operation $\circ$, such that $i \circ a = a \circ i = a$ for all $a \in S$
- For each $a \in S$, there exists an **inverse** element $a^{-1} \in S$, such that $a \circ a^{-1} = a^{-1} \circ a = i$

Commutative group

- A group $G = (S, \circ)$ is considered to be **commutative** if, in addition to the aforementioned four required properties, the group possesses the following property:

  $a \circ b = b \circ a$ for all $a, b \in S$

Group: example

- The additive group ($\mathbb{Z}$, +) has all four required properties:
- **Closure**: $a + b = c \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$
- **Associativity**: $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{Z}$
- **Identity**: The additive identity element is 0, with $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$
- **Invertibility**: For all $a \in \mathbb{Z}$, the inverse element is $-a \in \mathbb{Z}$, with $a + (-a) = (-a) + a = 0$
- Furthermore, the additive group ($\mathbb{Z}$, +) is **commutative**, since $a + b = b + a$ for all $a, b \in \mathbb{Z}$

Group: other examples

- The set of integers $\mathbb{Z}_m = \{0, 1, \ldots, m\text{-}1\}$ and the operation *addition modulo m* form a group $(\mathbb{Z}_m, +)$ with the additive identity element 0.
  - This group possesses all four required properties; in particular, every element a has an inverse $-a$ such that $a + (-a) \equiv 0 \bmod m$

- $(\mathbb{R}, +)$ is a group as well

Group: counterexample

- $(\mathbb{Z}, \cdot)$ is **not** a group, because it does not meet the requirement for the **invertibility** property
  - The multiplicative inverse does **not** exist for most elements in $\mathbb{Z}$, i.e. for most elements $a \in \mathbb{Z}$, the inverse multiplicative element a^{-1} does **not** exist, such that $a \cdot a^{-1} = 1$

- Similarly, the set $\mathbb{Z}_m$ does **not** form a group with the operation multiplication *modulo m*, i.e. $(\mathbb{Z}_m, \cdot)$ is **not** a group, because most elements of the set do not have an inverse such that $a \cdot a^{-1} \equiv 1 \mod m$ (where 1 is the multiplicative identity element)

Order of a finite group

- We have seen sets with an infinite number of elements, such as $\mathbb{Z}$ and $\mathbb{R}$
- In cryptography, we are generally more interested in sets with a finite number of elements (i.e. finite sets) such as the set $\mathbb{Z}_m$, which has m elements
- The order $|G|$ of a finite group G is the number of elements in G

- E.g. the order of the group $G = (\mathbb{Z}_m, +)$ is $|G| = |\mathbb{Z}_m| = m$

Order of an element in a finite group

- The order $ord(a)$ of an element $a \in S$ in a group $G = (S, \circ)$ is the smallest positive integer k, such that

  $$a^k = \underbrace{a \circ a \circ a \ldots a \circ a}_{k \text{ times}} = i,$$

  where $i \in S$ is the identity element with respect to the operation $\circ$

- E.g.
  - The order of the element 1 in $G = (\mathbb{Z}_6, +) = (\{0, 1, 2, 3, 4, 5\}, +)$ is 6, since $1^6 = 1 + 1 + 1 + 1 + 1 + 1 \equiv 0 \mod 6$, with element 0 being the identity element
  - The order of the identity element 0 in $G = (\mathbb{Z}_6, +)$ is 1, since $0^1 \equiv 0 \mod 6$
  - The order of the element 2 in $G = (\mathbb{Z}_6, +)$ is 3, since $2^3 = 2 + 2 + 2 \equiv 0 \mod 6$
  - The order of the element 1 in $G = (\mathbb{Z}_m, +)$ is m

Ring: definition

- A ring is a group (S, ○, *) that has a second operation *, with the following requirements on *:

- The operation * must be **closed**, i.e. $a * b = c \in S$ for all $a, b \in S$
- The operation * must be **associative**, i.e. $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$
- There must be an **identity** element $i' \in S$ with respect to the operation *, such that $i' * a = a * i' = a$ for all $a \in S$
- The operation * must be **distributive** over the operation ○
- *Note: there is no invertibility requirement on the operation **

Distributivity: definition

- Suppose there are two associative operations ○ and * that operate on elements of a set *S*. The operation * is **distributive** over the operation ○, if and only if $a * (b \circ c) = (a * b) \circ (a * c)$ for all $a, b, c \in S$
- E.g.
  - For the set of all integers $\mathbb{Z}$, the multiplication operation '·' is distributive over the addition operation '+'
  - Conversely, for the set of all integers $\mathbb{Z}$, the addition operation '+' is **not** distributive over the multiplication operation '·'

Integer rings

- The integer ring is an important example of a ring

- The integer ring $(\mathbb{Z}_m, +, \cdot)$ consists of:

1. The finite set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m\text{-}1\}$
2. Two operations '+' and '·' for all $a, b \in \mathbb{Z}_m$ such that:

   $a + b \equiv c \bmod m, \ (c \in \mathbb{Z}_m)$

   $a \cdot b \equiv d \bmod m, \ (d \in \mathbb{Z}_m)$

Integer rings: properties

- The ring is said to be *closed*
  - i.e. We can add and multiply any two numbers of the ring and the result is always in the ring
- Addition and multiplication are associative, i.e. $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{Z}_m$
- The distributive law holds for a ring, i.e. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in \mathbb{Z}_m$
- There is an identity element 0 with respect to <u>addition</u>, i.e. for every element $a \in \mathbb{Z}_m$, it holds that $a + 0 \equiv a \bmod m$
- For every element a in the ring, there is always a negative element $-a$ such that $a + (-a) \equiv 0 \bmod m$; in other words, the *additive inverse* always exists

Integer rings: properties

- There is an identity element 1 with respect to <u>multiplication</u>, i.e. for every element $a \in \mathbb{Z}_m$, it holds that $a \cdot 1 \equiv a \bmod m$
- The *multiplicative inverse* exist for some, but **not** all, elements in the ring. For $a \in \mathbb{Z}_m$, if the multiplicative inverse exists, then the inverse of a is defined as a^{-1}, such that $a \cdot a^{-1} \equiv 1 \bmod m$
  - Also, if the multiplicative inverse of a exists, then we can divide some element $b \in \mathbb{Z}_m$ by a, since $b / a \equiv b \cdot a^{-1} \bmod m$
  - The multiplicative inverse of $a \in \mathbb{Z}_m$ exists if and only if $gcd(a, m) = 1$, i.e. a and m are coprime
  - E.g. The multiplicative inverse of 15 exists in $\mathbb{Z}_{26}$, since $gcd(15, 26) = 1$; conversely, the multiplicative inverse of 12 does not exist in $\mathbb{Z}_{26}$ because $gcd(12, 26) = 2$

Field: definition

- A field $F = (S, +, \cdot)$ is a ring with the following properties:
- All elements of S form an additive group with the group operation '+' and the identity element 0
- All elements of S, except the element 0, form a multiplicative group with the group operation '·' and the identity element 1
  - Particularly, each non-zero element has a multiplicative inverse
- When the two group operations are mixed, the operation '·' is distributive over the operation '+', i.e. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in S$

GCD(7469, 2464)

$7469 = 2464(3) + 77$

$2464 = 77(36) + 0$

$\gcd = 77$

GCD(2689, 4001)

$4001 = 2689(1) + 1312$

$2689 = 1312(2) + 65$

2624

$1312 = 65(20) + 12$

$65 = 12(5) + 5$

$12 = 5(2) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

$\gcd = 1$

GCD(1109, 4999)

$4999 = 1109(4) + 563$

$1109 = 563(1) + 546$

$563 = 546(1) + 17$

$546 = 17(32) + 2$

$17 = 2(8) + 1$

$2 = 1(2) + 0$

$\gcd = 1$

gcd(15, 26)

$26 = 15(1) + 11$

$15 = 11(1) + 4$

$11 = 4(2) + 3$

$4 = 3(1) + 1$

$3 = 1(3) + 0$

$\gcd = 1$

$1 = 4 - 1(3)$

$1 = 4 - (11 - 2(4))$

Field: example

- $(\mathbb{R}, +, \cdot)$ is a field with the identity element 0 for the additive group and the identity element 1 for the multiplicative group
- Every real number *a* has an additive inverse -*a*, and every non-zero real number *a* has a multiplicative inverse 1/*a*

Rings vs. fields

- A ring is a generalization of a field (i.e. all fields are rings, but not all rings are fields)
- Stricter requirements are imposed on fields:
  - All non-zero elements of a field **must** have a **multiplicative inverse**; whereas for a ring, a non-zero element is not required to have a multiplicative inverse
  - The multiplication operation of a field **must** be **commutative**, but the multiplication operation of a ring does not need to be commutative

Finite fields (Galois fields)

- In cryptography, we are usually interested in fields with a finite number of elements
  - These fields are known as finite fields or Galois fields
- The number of elements in the field is called the *order* of the field (similar to the order of a finite group)

- The following theorem regarding finite fields is fundamental:

  A field with order m only exists if m is a prime power, i.e. $m = p^n$ for some positive integer n and prime integer p. p is called the characteristic of the finite field.

Finite fields (Galois fields)

- The implication of the theorem is that there are finite fields with 5 elements, or with 49 elements (since $7^2 = 49$), or with 256 elements (since $2^8 = 256$)
- By contrast, there is no finite field with 36 elements, since 36 is not a prime power ($2^2 \cdot 3^2 = 36$)

Prime fields

- A prime field *GF*(*p*) is a Galois (finite) field of prime order (i.e. $n = 1$)
- The two operations of the field are integer addition *modulo p* and integer multiplication *modulo p*

- The following important theorem defines a prime field:

  Let *p* be a prime integer. The integer ring $\mathbb{Z}_p$ is denoted as *GF*(*p*) and is referred to as a prime field, or as a Galois field with a prime number of elements. All non-zero elements of *GF*(*p*) have an inverse. Arithmetic in *GF*(*p*) is done *modulo p*.

Prime fields: examples

- Prime field *GF*(5):
  - The tables below show how to add or multiply (*modulo* 5) any two elements in *GF*(5), as well as the additive and multiplicative inverses

addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

additive inverse

$-0 = 0$
$-1 = 4$
$-2 = 3$
$-3 = 2$
$-4 = 1$

multiplication

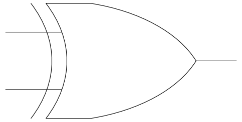
×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

multiplicative inverse

0^{-1} does not exist
$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

Prime fields: examples

- Prime field *GF*(2):
  - This is a very important prime field (the smallest possible finite field)
  - Addition and multiplication are calculated *modulo* 2, as shown in the tables below:

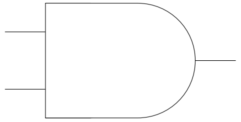


addition

$+$	0	1
0	0	1
1	1	0

multiplication

$\times$	0	1
0	0	0
1	0	1



  - Addition *modulo* 2 is the XOR operation (likewise for subtraction *modulo* 2)
    - i.e. XOR operation is addition or subtraction in the Galois field *GF*(2)
  - Multiplication *modulo* 2 is the AND operation
    - i.e. AND operation is multiplication in the Galois field *GF*(2)

Integer addition *modulo p* computation

- How to compute *a* + *b mod p*, which is addition in *GF*(*p*)
  - "Official" way: Add the two integers *a* and *b*, then do an integer divide by the modulus *p* (a prime number), and keep only the remainder
  - *Practically*, this means you first add the two integers *a* and *b* as you would for normal arithmetic, then subtract the closest integer multiple of *p* (that is less than or equal to the sum of *a* and *b*) from the result – this gives you the remainder
  - Note: "*a* + *b mod p*" is the same as "(*a* + *b*) *mod p*"
- E.g. addition in *GF*(5)
  - To compute 4 + 3 *mod* 5, add 4 and 3 to obtain 7, then subtract 5, which is the closest integer multiple of 5 that is less than or equal to 7 – we obtain 2
  - Thus 4 + 3 *mod* 5 = 2 *mod* 5
  - This result is consistent with the addition table for *GF*(5)

Integer multiplication *modulo p* computation

- How to compute $a \cdot b \ mod \ p$, which is multiplication in $GF(p)$
  - "Official" way: Multiply the two integers a and b, then do an integer divide by the modulus p, and keep only the remainder
  - *Practically*, this means you first multiply the two integers a and b as you would for normal arithmetic, then subtract the closest integer multiple of p (that is less than or equal to the product of a and b) from the result – this gives you the remainder
- E.g. multiplication in $GF(5)$
  - To compute $4 \cdot 3 \ mod \ 5$, multiply 4 by 3 to obtain 12, then subtract 10, which is the closest integer multiple of 5 that is less than or equal to 12; we obtain 2
  - Thus $4 \cdot 3 \ mod \ 5 = 2 \ mod \ 5$
  - This result is consistent with the multiplication table for $GF(5)$

Extension fields

- An extension field is a Galois (finite) field $GF(p^n)$ with $n > 1$
- The order of an extension field is **not** prime (since $m = p^n$ is not prime)
  - This means that **if** we were to represent the elements of $GF(p^n)$ as **integers**, not all non-zero integers of $GF(p^n)$ will have an **inverse**
  - This consequently implies that we **cannot** perform **integer** addition and multiplication ***modulo*** $\boldsymbol{p^n}$ on the elements of an extension field
  - Rather, we need to represent the elements of an extension field using a different notation (i.e. not integers, but *polynomials* instead) and implement different rules for performing arithmetic on these elements

Extension fields

- We can roughly think of an extension field $GF(p^n)$ as an algebraic structure that contains n “instances” of a prime field $GF(p)$

- The elements of an extension field $GF(p^n)$ are not represented by integers
- Rather, the elements of $GF(p^n)$ are represented by *polynomials* of degree n-1 with coefficients in the prime field $GF(p)$
- Arithmetic in the extension field is achieved by performing a certain kind of *polynomial arithmetic*:
    - Addition and subtraction: bitwise XOR of the corresponding coefficients
    - Multiplication: polynomial multiplication and reduction by a fixed *irreducible polynomial*

Extension fields: example – $GF(2^8)$

- The extension field $GF(2^8)$ is used in the layers of AES (this field was chosen because each of the field elements can be represented by one byte)
- Each element in $GF(2^8)$ is represented by a polynomial of the form:

  $A(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, $a_i \in GF(2) = \{0, 1\}$

- E.g. byte 0xC3 = 11000011_2 can be represented as: $A(x) = x^7 + x^6 + x + 1$
- Note that the factors x^7, x^6, etc. are placeholders (and are not the variables to be evaluated); we do **not** need to store these factors since each polynomial $A(x)$ can be stored in digital form as an 8-bit vector:

  $A = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$

Extension fields: polynomial arithmetic

- We will discuss the following polynomial arithmetic operations for extension fields $GF(2^n)$ with $p = 2$, particularly for $GF(2^8)$, in the next lecture:
  - Addition
  - Subtraction
  - Multiplication
  - Division
  - Inversion (multiplicative inverse)