INFORMATION SECURITY

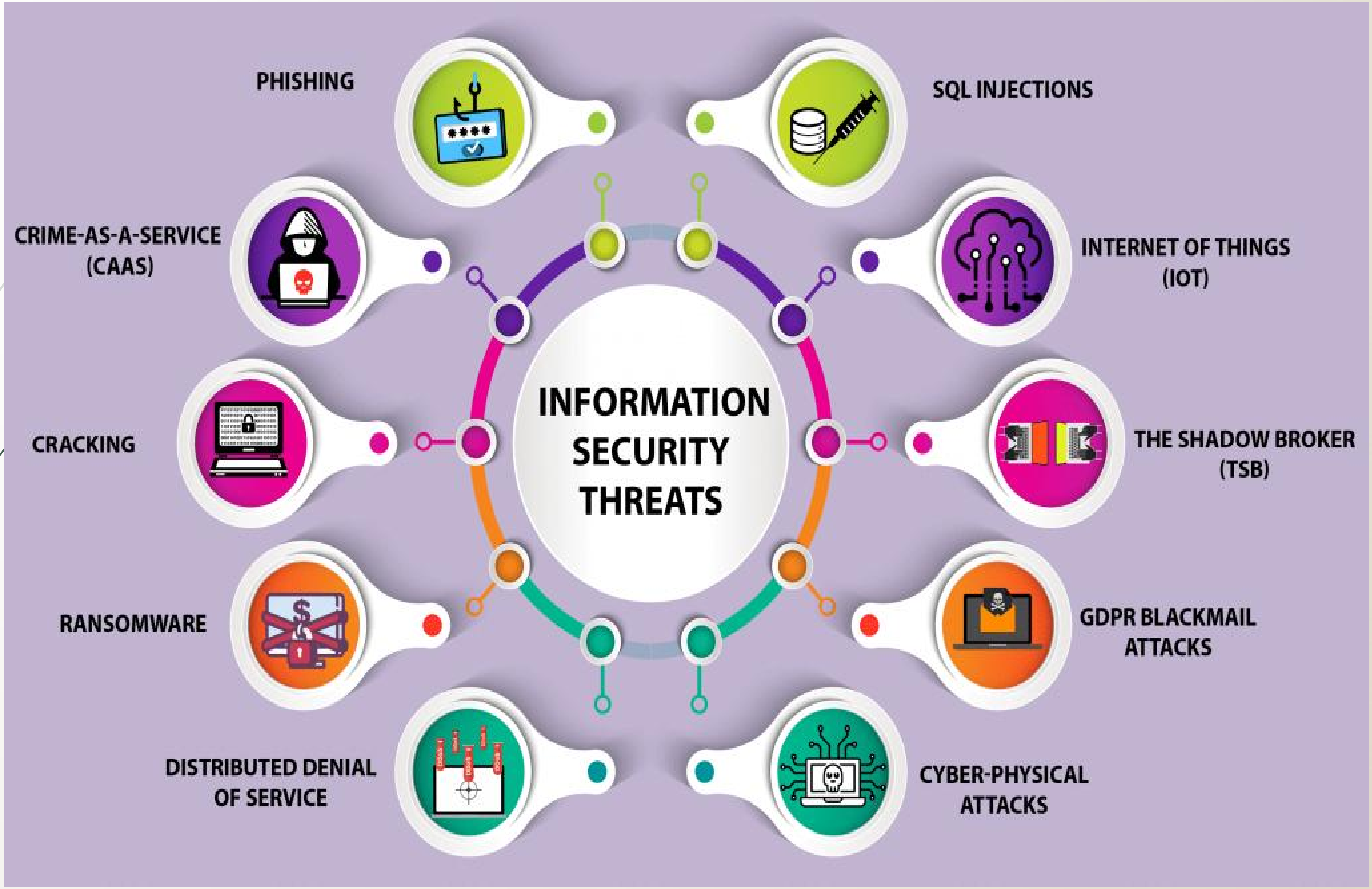
Three Pillars of Information Security

- Confidentiality
- Integrity
- Availability
- Non repudiation
- Authenticity
- Accountability

Triads of Confidentiality

- **Confidentiality** - means information is not disclosed to unauthorized individuals, entities and process
- **Integrity** - means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way.
- **Availability** -means information must be available when needed.
- **Non repudiation –** means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. Data Integrity and Authenticity are pre-requisites for Non repudiation.
- **Authenticity –** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.
- **Accountability –** means that it should be possible to trace actions of an entity uniquely to that entity.

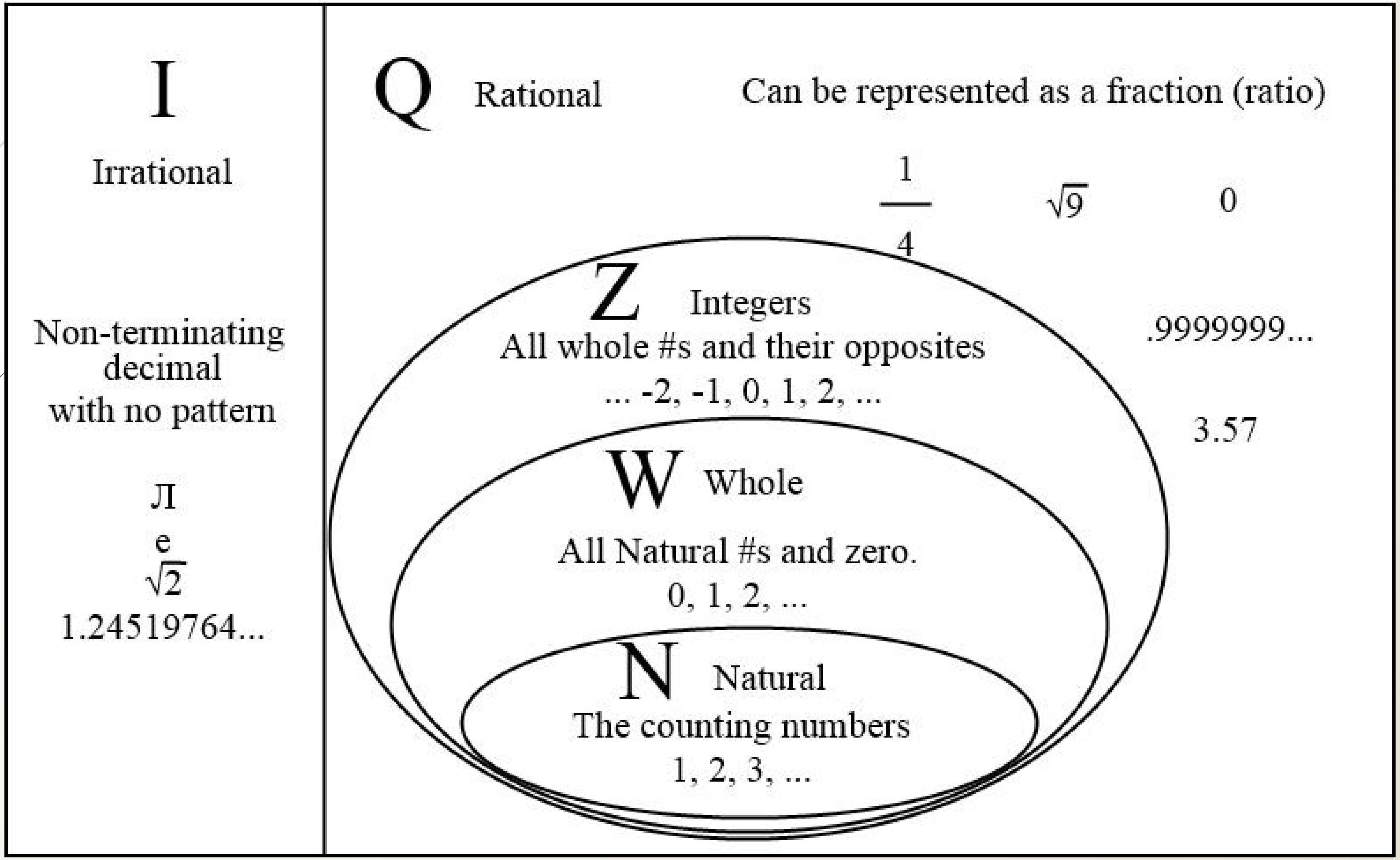

Information Security?
Computer Security?
IT Security?
Cybersecurity?


PHISHING
SQL INJECTIONS
CRIME-AS-A-SERVICE (CAAS)
INTERNET OF THINGS (IOT)
CRACKING
INFORMATION SECURITY THREATS
THE SHADOW BROKER (TSB)
RANSOMWARE
GDPR BLACKMAIL ATTACKS
DISTRIBUTED DENIAL OF SERVICE
CYBER-PHYSICAL ATTACKS

NUMBERS

$\mathbb{N}$	$\mathbf{W}$	$\mathbb{Z}$	$\mathbb{Q}$
NATURAL	WHOLE	INTEGERS	RATIONAL

Real Numbers



The Structure of $+$ and $\times$ on $\mathbb{Z}$

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto a + b \end{aligned}$$

$$\begin{aligned} \times : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto a \times b \end{aligned}$$

Properties of +:

- (Associativity): $a + (b + c) = (a + b) + c \; \forall a, b, c \in \mathbb{Z}$
- (Existence of additive identity) $a + 0 = 0 + a = a \; \forall a \in \mathbb{Z}$.
- (Existence of additive inverses) $a + (-a) = (-a) + a = 0 \; \forall a \in \mathbb{Z}$
- (Commutativity) $a + b = b + a \; \forall a, b \in \mathbb{Z}$.

The Structure of $+$ and $\times$ on $\mathbb{Z}$

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a,b) &\mapsto a+b \end{aligned}$$

$$\begin{aligned} \times : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a,b) &\mapsto a \times b \end{aligned}$$

Properties of x:

- (Associativity): $a \times (b \times c) = (a \times b) \times c \; \forall a, b, c \in \mathbb{Z}$
- (Existence of multiplicative identity) $a \times 1 = 1 \times a = a \; \forall a \in \mathbb{Z}$.
- (Commutativity) $a \times b = b \times a \; \forall a, b \in \mathbb{Z}$.

The operations of $+$ and $\times$ interact by the following law:

- (Distributivity) $a \times (b + c) = (a \times b) + (a \times c) \; \forall a, b, c \in \mathbb{Z}$.

Properties of $\mathbb{Q}$

- All of the above hold for + and × on Q
- Also non-zero elements have multiplicative inverses:

Given $a \in \mathbb{Q}\backslash\{0\}$, $\exists b \in \mathbb{Q}$ such that $ab = ba = 1$.

Properties of $\mathbb{Z}$

- a, b ∈ Z such that ab = 0 ⇒ either a = 0 or b = 0 ⇒. Z is an integral domain

Cancellation Law: For $a, b, c \in \mathbb{Z}$, $ca = cb$ and $c \neq 0 \Rightarrow a = b$.

PROPERTIES OF NUMBERS

1. $5 \times 0 = 0$
2. $(6 \times 4) + (6 \times 11) = 6 \times (4 + 11)$
3. $4 + 9 = 9 + 4$
4. $(6 + 2) + 8 = 6 + (2 + 8)$
5. $27 + 0 = 27$
6. $36 \times 1 = 36$
7. $(9 \times 8) \times 15 = 9 \times (8 \times 15)$
8. $17 \times 33 = 33 \times 17$
9. $(2 \times 7) \times 4 = 2 \times (7 \times 4)$
10. $(5 + 3) + 9 = 5 + (3 + 9)$
11. $2 \times (3 + 7) = (2 \times 3) + (2 \times 7)$
12. $4 + (6 + 3) = 4 + (3 + 6)$
13. $48 \times 0 = 0$
14. $51 \times 30 = 30 \times 51$

Abstract Algebra

- Branch of mathematics
- Algebraic concepts are generalized by using symbols
- Represent basic arithmetical operations
- Abstract algebra - set of advanced topics of algebra that deal with abstract algebraic structures
- Groups, rings, and fields.

GROUPS $(G, *)$.

Let G be a set. A ***binary operation*** is a map of sets:

$$*: G \times G \to G.$$

$$*(a, b) = a * b \ \forall a, b \in G.$$

Fundamental Definition. *A* ***group*** *is a set G, together with a binary operation $*$, such that the following hold:*

1. *(Associativity):* $(a * b) * c = a * (b * c) \ \forall a, b, c \in G$.
2. *(Existence of identity):* $\exists e \in G$ *such that* $a * e = e * a = a \ \forall a \in G$.
3. *(Existence of inverses):* *Given* $a \in G, \exists b \in G$ *such that* $a * b = b * a = e$.

- Examples: (Z, +), (Q, +), (Q\{0}, ×), (Z/mZ, +), and (Z/mZ \ {[0]}, ×) if m is prime.
- (Z, ×) is not a group.

PERMUTATION GROUP

- A permutation of a set X is a function σ : X → X that is one-to-one and onto.

Example Consider a set X containing 3 objects, say a triangle, a circle and a square. A permutation of $X = \{\triangle, \circ, \square\}$ might send for example

$$\triangle \mapsto \triangle,\ \circ \mapsto \square,\ \square \mapsto \circ,$$

and we observe that what just did is exactly to define a bijection on the set X, namely a map $\sigma : X \to X$ defined as

$$\sigma(\triangle) = \triangle,\ \sigma(\circ) = \square,\ \sigma(\square) = \circ.$$

Example can then be rewritten as $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ such that

$$\sigma(1) = 1,\ \sigma(2) = 3,\ \sigma(3) = 2,\ \text{or } \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Permutation Group

$$\alpha_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \alpha_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \alpha_3 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix},$$

$\alpha_1 0 \alpha_2 = \alpha_2, \alpha_1 0 \alpha_3 = \alpha_3,$

The complete table:

$\oplus$	α_1	α_2	α_3
α_1	α_1	α_2	α_3
α_2	α_2	α_3	α_1
α_3	α_3	α_1	α_2

- Closure holds
- $\oplus$ is associative
- α_1 is the identity element
- each element has its inverse like. $\alpha_1^{-1} = \alpha_1, \alpha_2^{-1} = \alpha_3, \alpha_3^{-1} = \alpha_2,$

$\therefore (S, \oplus)$ forms a finite abelian group of order 3

$$\alpha_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \alpha_3 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

Commutativity property

ABELIAN GROUPS $(G, *)$.

Definition. *A group $(G, *)$ is called* **Abelian** *if it also satisfies*

$$a * b = b * a \; \forall a, b \in G.$$

This is also called the commutative property.

The fundamental Abelian group is $(\mathbb{Z}, +)$.

Closure - $a, b \in Z \Rightarrow a + b \in Z$

Associative $\rightarrow a + (b + c) = (a + b) + c, \; a, b, c \in Z$

Identity element exists $\rightarrow a + 0 = 0 + a = a, \; a, 0 \in Z$

Inverse Element exists $\Rightarrow a + (-a) = (-a) + a = 0 \quad a, -a, \in Z$

Commutativity $\rightarrow a + b = b + a, \; a, b \in Z$.

Hence $(Z, +)$ is abelian.

Prove that x*y = x+y+k is an abelian group on set R of real numbers, where k is a fixed constant.

Closure:

$x*y=x+y+k$ (k is a fixed constant), on the set RR of the real numbers.

$x*y=x+y+k=y+x+k=y*x$. Commutativity holds.

$(x*y)*z=(x+y+k)*z=(x+y+k)+z+k=(z+y+k)+x+k=x*(y*z)$. Associativity holds.

$x*e=x+e+k=x$, so $e=-k$.
Further, $e*x=-k+x+k=x$. Thus e is an identity.

$x*x'=x+x'+k=e$, so $x'=e-x-k$.
Further, $x'*x=e-x-k+x+k=e$. Thus, x' is an inverse element.
This set is an Abelian Group.

Prove that $x*y = x+y+k$ is an abelian group on set R of real numbers, where k is a fixed constant.

Prove that $x * y = \frac{xy}{2}$, on the set $\{x \in \mathbb{R} : x \neq 0\}$ is an abelian group

$x * y = \frac{xy}{2} = \frac{yx}{2} = y * x$. Commutativity holds.

$(x * y) * z = (\frac{xy}{2}) * z = \frac{(xy)z}{2} = \frac{x(yz)}{2} = x * (y * z)$. Associativity holds.

$x * e = \frac{xe}{2} = x$, so $e = 2$. Further, $e * x = \frac{2x}{2} = x$. Also, $e = 0$, but this identity doesn't hold for the elements in the domain. Thus, e is an identity.

$x * x' = \frac{xx'}{2} = e$, so $x' = \frac{2e}{x}$. Further, $x' * x = \frac{\frac{2e}{x} x}{2} = e$. Inverse exists.

This set is an Abelian Group.

Cyclic groups $(G, *)$.

Definition. *A group* $(G, *)$ *is said to be cyclic if* $\exists x \in G$ *such that* $gp(\{x\}) = G$, *i.e.* G *can be generated by a single element. In concrete terms this means that* $G = \{x^n | n \in \mathbb{Z}\}$.

Example: ({1,-1,i,-i},x)

Each element can be written as a power of *a* in multiplicative notation, or as a multiple of *a* in additive notation. This element *a* is called the *generator* of the group.

- Closure
- Associativity
- Identity
- Inverse
- Generator

Consider binary relation * defined on set A={A,B,C,D} by following table and check commutative and Associative

*	A	B	C	D
A	A	C	B	D
B	D	A	B	C
C	C	D	A	A
D	D	B	A	C

Commutative

Associative

RINGS

Definition. *A **ring** is a set R with two binary operations, $+$, called addition, and $\times$, called multiplication, such that:*

1. *R is an **Abelian group** under addition.*
2. *R is a **monoid** under multiplication (inverses do not necessarily exist).*
3. *$+$ and $\times$ are related by the distributive law:*

$$(x + y) \times z = x \times z + y \times z \text{ and } x \times (y + z) = x \times y + x \times z \; \forall x, y, z \in R$$

The identity for $+$ is "zero", denoted 0_R (often just written as 0), and the identity for $\times$ is "one", denoted 1_R (often just written as 1).

Example: The integers under the usual addition and multiplication (Z, x, +).

Set of n-square matrices over Real numbers

Commutative Ring: $a \cdot b = b \cdot a$ for all a, b in R, Eg: Z_n , arithmetic operations Modulo n

INTEGRAL DOMAIN

An *integral domain* is a nonzero commutative ring in which the product of any two nonzero elements is nonzero.

A commutative Ring that follows the axioms:

- Multiplicative identity: There is an element 1 in R such that a1 = 1a = a for all a in R.
- No zero divisors: If a, b in R and ab = 0, then either a = 0 or b = 0.

Example:

The commutative ring $Z_5 = \{0,1,2,3,4\}$ is an integral domain.

For every x, y in Z_5, $x \otimes_5 y$ is not equal to zero. This implies that $x \neq 0$ and $y \neq 0$. That is,

$2 \otimes_5 3 = 1$

$4 \otimes_5 2 = 3$

$3 \otimes_5 0 = 0$

FIELDS

Definition A **field** is a nonempty set F of elements with two operations "+" and "x" satisfying the following axioms.

$\forall a, b, c \in F$

(i) F is closed under + and x i.e., a+b and a x b are in F.

(ii) Commutative laws: a+b=b+a, a x b=b x a

(iii) Associative laws: (a+b)+c=a+(b+c) , (a x b) x c=a x (b x c)

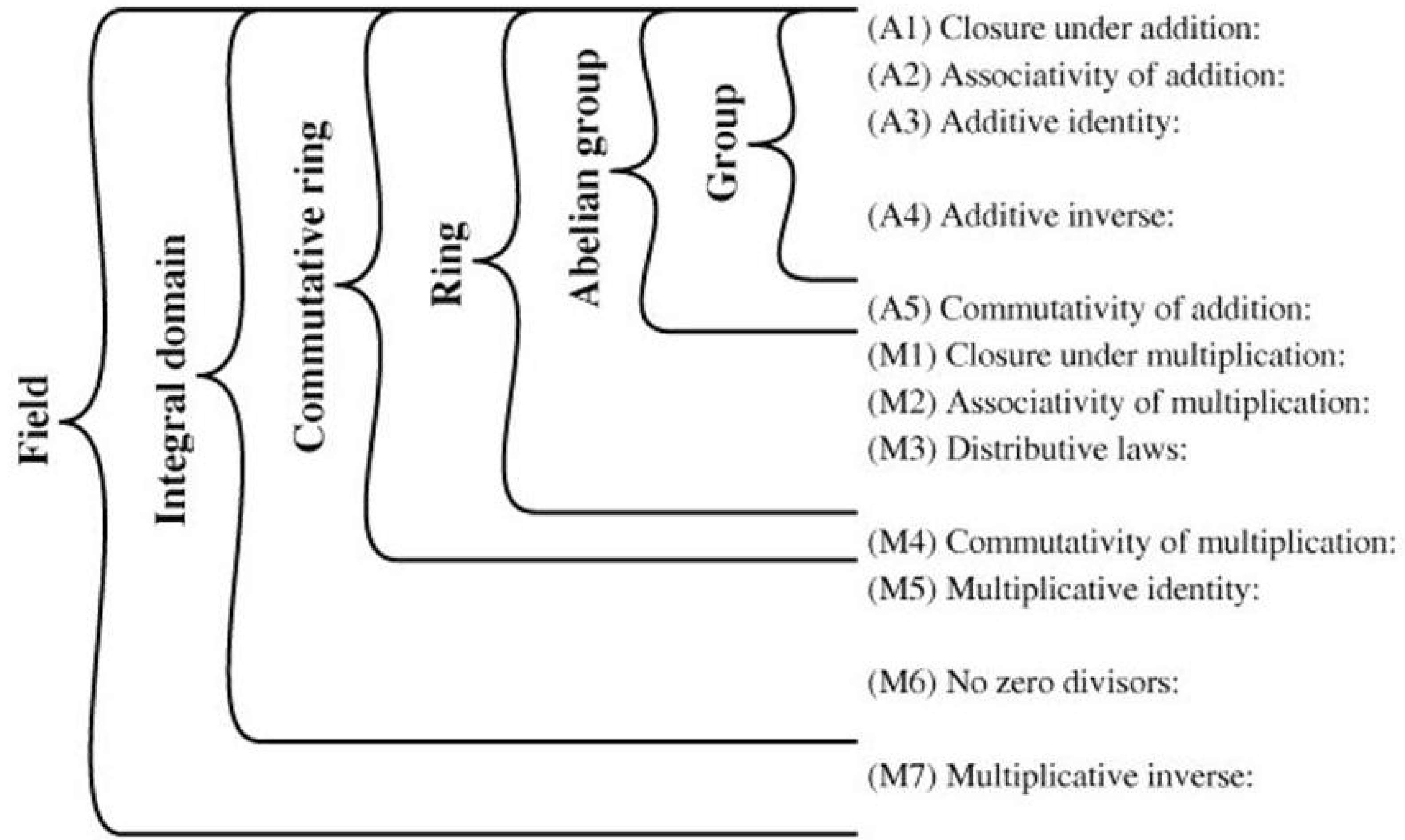
(iv) Distributive law: a x(b+c) = a x b + a x c

(v) (vi) Identity: a+0 = a , a x 1 = a for all a $\in$ F. 0 x a = 0.

(vii) Additive inverse: for all a $\in$ F, there exists an additive inverse (-a) such that a+(-a)=0

(viii) Multiplicative inverse: for all a F, $a \neq 0$, there exists a multiplicative inverse a^{-1} such that a x a^{-1}=1

Group, Ring, and Field



INTRODUCTION TO NUMBER THEORY

DIVISIBILITY :

Definition: Let $a, b \in \mathbb{Z}$, with $a \neq 0$. We say "a **divides** b" if there exists $m \in \mathbb{Z}$ such that $b = ma$.

- a|b => a divides b

Examples: We have $1 \mid 6$, $2 \mid 6$, $-2 \mid 6$, $6 \mid 6$, $6 \nmid 3$, $6 \mid 0$. However, neither $0 \mid 6$ nor $0 \nmid 6$ make sense since divisibility by 0 is not defined.

Properties:

- **Transitivity:** If $a \mid b$ and $b \mid c$, then $a \mid c$.
- **Sums/differences:** If $d \mid a$ and $d \mid b$, then $d \mid a + b$ and $d \mid a - b$.
- **Linear combinations:** If $d \mid a$ and $d \mid b$, then, for any $x, y \in \mathbb{Z}$, $d \mid ax + by$.

Divisors

- say a non-zero number b **divides** a if for some m have a=mb (a,b,m all integers)
- that is b divides into a with no remainder
- denote this b|a
- and say that b is a **divisor** of a
- eg. all of 1,2,3,4,6,8,12,24 divide 24

DIVISION ALGORITHM

Given any positive integer n and any integer a, if we divide a by n , we get an integer quotient, q and integer remainder r that obey the following relationship:

$$a = qn + r,\ 0 < r < n;\ q = a/n$$

Example:

$a = 11,\ n = 7 \Rightarrow 11 = 1 \times 7 + 4$ i.e. $q = 1,\ r = 4$

$a = -11,\ n = 7 \Rightarrow -11 = (-2)\,7 + 3$ i. e $q = -2,\ r = 3$

Modular Arithmetic

- Modulo is the operation of finding the **Remainder** when you divide two numbers.
- define **modulo operator** "a mod n" to be remainder when a is divided by n
- r is called a **residue** of a mod n
  - since with integers can always write: $a = qn + r$ => $a = qn + (a \bmod n)$
  - usually chose smallest positive remainder as residue
    - ie. $0 <= r <= n-1$
    - Eg: 11mod 7 = 4 & -11 mod 7 = 3
- Two integers are said to be *congruent modulo n*,
- if (a mod n) = (b mod n) => **a $\equiv$ b (mod n)**
  - when divided by *n,* a & b have same remainder
  - eg. $100 \equiv 34 \bmod 11$
- **modulo reduction**
  - eg. $-12 \bmod 7 \equiv -5 \bmod 7 \equiv 2 \bmod 7 \equiv 9 \bmod 7$

Greatest Common Divisor (GCD)

- GCD (a,b) of a and b is the largest number that divides evenly into both a and b
  - eg GCD(60,24) = 12
- When we have **no common factors** (except 1), the numbers are **relatively prime**
  - eg GCD(8,15) = 1
  - hence 8 & 15 are relatively prime

Euclidean Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - GCD(a,b) = GCD(b, a mod b)
- Euclidean Algorithm to compute GCD(a,b) is:

EUCLID(a,b)

1. A = a; B = b
2. if B = 0 return A = gcd(a, b)
3. R = A mod B
4. A = B
5. B = R
6. goto 2

Example GCD(1970,1066)

1970 = 1 x 1066 + 904 gcd(1066, 904)
1066 = 1 x 904 + 162 gcd(904, 162)
904 = 5 x 162 + 94 gcd(162, 94)
162 = 1 x 94 + 68 gcd(94, 68)
94 = 1 x 68 + 26 gcd(68, 26)
68 = 2 x 26 + 16 gcd(26, 16)
26 = 1 x 16 + 10 gcd(16, 10)
16 = 1 x 10 + 6 gcd(10, 6)
10 = 1 x 6 + 4 gcd(6, 4)
6 = 1 x 4 + 2 gcd(4, 2)
4 = 2 x 2 + 0 gcd(2, 0)

Hence gcd(1970,1066) = 2

PROPERTIES OF CONGRUENT MODULO

The Congruent modulo operator has the following properties:

1. $a \equiv b \bmod n$ if $n|(a-b)$.
2. $a \equiv b \bmod n$ implies $b \equiv a \bmod n$. Symmetric Property
3. $a \equiv b \bmod n$ and $b \equiv c \bmod n$ imply $a \equiv c \bmod n$. Transitive Property
4. $a \equiv a \pmod{n}$. Reflexive Property

$23 \equiv 8 \pmod 5$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \pmod 8$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 \pmod{27}$	because	$81 - 0 = 81 = 27 \times 3$

Properties of Modular Arithmetic

1. Addition property: $(a+b) \bmod n = [a \bmod n + b \bmod n] \bmod n$

2. Subtraction property: $(a-b) \bmod n = [a \bmod n - b \bmod n] \bmod n$

3. Multiplication property: $(a \times b) \bmod n = [a \bmod n \times b \bmod n] \bmod n$

4. Division property: $\frac{a}{k} \equiv \frac{b}{k}\left(\bmod \frac{n}{\gcd(n,k)}\right)$

5. Exponent property: $p^k \equiv q^k \pmod{n}$

$a^k(\text{mod}n)=(a(\text{mod}n))^k$

To find 11^7 mod 13, we can proceed as follows:
$11^2 = 121 \equiv 4 \pmod{13}$
$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$
$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

$Z_8 = \{0,1,2,3,4,5,6,7\}$ is a set of residues or residue classes (mod 8)

Addition Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication Modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Additive and multiplicative inverses modulo 8

Properties of Modular Arithmetic for Integers in Zn

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse ($-w$)	For each $w \in Z_n$, there exists a z such that $w + z = 0 \bmod n$

if $(a + b) \equiv (a + c) \pmod{n}$ **then** $b \equiv c \pmod{n}$

(5 + 23) ≡ (5 + 7)(mod 8}; 23 ≡ 7 (mod 8)

If (axb)$\equiv$ (axc)(mod n) **then** b $\equiv$ c (mod n), if **a** is relatively prime to **n.**

$6 \times 3 = 18 \equiv 2 \pmod 8$

$6 \times 7 = 42 \equiv 2 \pmod 8$

Yet $3 \not\equiv 7 \pmod 8$.

With $a = 6$ and $n = 8$,

Z_8	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

if we take $a = 5$ and $n = 8$, whose only common factor is 1,

Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

FIELDS

Galois Fields

- Examples of field: R, C, Q ;
- Z is not a field coz no inverse for all elements.
- Fields => Finite / Infinite
- A finite field is a field that contains a finite number of elements
- Finite fields play a key role in cryptography
- The number of elements in a finite field **must** be a power of a prime p^n
- known as Galois fields
- denoted $GF(p^n)$
- in particular often use the fields: $GF(p)$, $GF(2^n)$

Galois Fields

The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1

Inverses

In this case, addition is equivalent to the exclusive-OR (XOR) operation, and multiplication is equivalent to the logical AND operation.

- **GF(p)** is the set of integers {0,1, … , p-1} with arithmetic operations **modulo prime p**
- These form a finite field since have multiplicative inverses
- Hence arithmetic is "well-behaved" and can do addition, subtraction, multiplication, and division without leaving the field GF(p)

GF(7) Multiplication Example

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

This is a field of order 7 using modular arithmetic modulo 7.

Property	
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z = 0 \bmod n$

Z8 using modular arithmetic modulo 8, is not a field

Extended Euclidean Algorithm

The Extended Euclidean Algorithm computes the gcd(a,b) and also the values of integers x and y that satisfies the relation

$$ax + by = d = \gcd(a,b)$$

If a & b are relatively prime to each other, gcd(a,b) = 1

$$\Rightarrow ax + by = 1$$

$$(ax + by) \bmod a = 1 \bmod a$$

$$\Rightarrow ((ax \bmod a) + (by \bmod a) \bmod a) = 1 \bmod a$$

$$\Rightarrow (0 + by \bmod a) \bmod a = 1 \bmod a$$

$$\Rightarrow by \bmod a = 1$$

$$by = 1 \bmod a$$

$$\Rightarrow y = b^{-1}$$

Finding Inverses

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1-QB1,A2-QB2,A3-QB3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	5	16	5	106	339	4
1	106	–339	4	–111	355	1

The Euclidean algorithm can be extended so that, in addition to finding gcd(m, b), if the gcd is 1, the algorithm returns the multiplicative inverse of b.

Polynomial Arithmetic

- use polynomials

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$

  - not interested in any specific value of x
- several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coefficients mod p (coeff in GF(p))
  - poly arithmetic with coeffs mod p (coeff in GF(p))

  and polynomials mod polynomial m(x) whose highest power is some integer n

1. Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg

  let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) - g(x) = x^3 + x + 1$

  $f(x) \text{ x } g(x) = x^5 + 3x^2 - 2x + 2$

  $f(x) \,/\, g(x) = (x+2)$, $r = x$

2. Polynomial Arithmetic with Modulo Coefficients

- Polynomials where coefficients are elements of some field F
- when computing value of each coefficient do calculation modulo some value
  - forms a polynomial ring
- could be modulo any prime
- but we are most interested in mod 2
  - ie all coefficients are 0 or 1
  - eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$$f(x) + g(x) = x^3 + x + 1$$

$$f(x) \times g(x) = x^5 + x^2$$

Polynomial Division

- can write any polynomial in the form:
  - $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if have no remainder say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or **prime**) polynomial
- arithmetic modulo of an irreducible polynomial forms a field

The polynomial $f(x) = x^4 + 1$ over GF(2) is reducible, because $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$

Polynomial GCD

- can find greatest common divisor for polys
  - $c(x) = \mathrm{GCD}(a(x), b(x))$ if $c(x)$ is the poly of greatest degree which divides both $a(x), b(x)$
- can adapt Euclid's Algorithm to find it:

EUCLID[$a(x)$, $b(x)$]

1. $A(x) = a(x)$; $B(x) = b(x)$
2. **if** $B(x) = 0$ **return** $A(x) = \gcd[a(x), b(x)]$
3. $R(x) = A(x) \bmod B(x)$
4. $A(x) = B(x)$
5. $B(x) = R(x)$
6. **goto** 2

Polynomial GCD

Find $\gcd[a(x), b(x)]$ for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$. First, we divide $a(x)$ by $b(x)$:

$$
\begin{array}{r|l}
 & x^2 + x \\
\hline
x^4 + x^2 + x + 1 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & \underline{x^6 \qquad\;\; + x^4 + x^3 + x^2} \\
 & \qquad x^5 \qquad\qquad\qquad\quad + x + 1 \\
 & \qquad \underline{x^5 \qquad\; + x^3 + x^2 + x \quad} \\
 & \qquad\qquad\qquad x^3 + x^2 \qquad + 1
\end{array}
$$

This yields $r_1(x) = x^3 + x^2 + 1$ and $q_1(x) = x^2 + x$.
Then, we divide $b(x)$ by $r_1(x)$.

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
x^3 + x^2 + 1 & x^4 \qquad\;\; + x^2 + x + 1 \\
 & \underline{x^4 + x^3 \qquad + x} \\
 & \qquad x^3 + x^2 \qquad + 1 \\
 & \qquad \underline{x^3 + x^2 \qquad + 1}
\end{array}
$$

This yields $r_2(x) = 0$ and $q_2(x) = x + 1$.
Therefore, $\gcd[a(x), b(x)] = r_1(x) = x^3 + x^2 + 1$.

3. Modular Polynomial Arithmetic

- can compute in field $GF(2^n)$
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- form a finite field
- can always find an inverse
  - can extend Euclid’s Inverse algorithm to find the inverse

Arithmetic in GF(2³)

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

		000	001	010	011	100	101	110	111
	×	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(c) Additive and multiplicative inverses

EXAMPLE GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Computational Considerations

- since coefficients are 0 or 1, can represent any such polynomial as a bit string
- addition becomes XOR of these bit strings
- multiplication is shift & XOR
  - cf long-hand multiplication
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift & XOR)

Computational Example

- in $GF(2^3)$ have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- so addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- and multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101){<<}1 \text{ XOR } (101){<<}0 =$
    $1010 \text{ XOR } 101 = 1111_2$
- polynomial modulo reduction (get q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$

USING A GENERATOR

- a **generator** g is an element whose powers generate all non-zero elements
  - in F have 0, $g^0, g^1, \ldots, g^{q-2}$
- can create generator from **root** of the irreducible polynomial
- then implement multiplication by adding exponents of

Generator for $GF(2^3)$ using $x^3 + x + 1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
$g^0 (= g^7)$	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Summary

- have considered:
  - concept of groups, rings, fields
  - modular arithmetic with integers
  - Euclid's algorithm for GCD
  - finite fields GF(p)
  - polynomial arithmetic in general and in $GF(2^n)$