Ring: R - Non-empty set.

Let $+$ & $\cdot$ be two binary operations.

Then $(R,+,\cdot)$ is called a ring if it satisfies the following properties:

1. $(R,+)$ is an abelian group.
2. $(R,\cdot)$ is associative. [$(R,\cdot)$ is a semi group]
3. Distributivity: '$\cdot$' is distributive over '$+$' from left as well as from right.

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \& \quad (a+b)\cdot c = (a\cdot c) + (b\cdot c) \quad \forall\, a,b,c\in R.$$

If '$\cdot$' is commutative (i.e $a\cdot b = b\cdot a \ \forall\, a,b\in R$) then $(R,+,\cdot)$ is called commutative ring.

If '$\cdot$' is commutative and identity w.r. to '$\cdot$' exists in R then $(R,+,\cdot)$ is called a commutative ring with unity.

$\{\because\ a\cdot b = b\cdot a \ \forall\, a,b\in R,\ \exists\ 1\in R$ s.t. $1\cdot a = a\cdot 1 = a \ \forall\, a\in R\}$

Ex:

$(\mathbb{Z},+,\cdot)$	: Commutative	ring	with	unity.
$(\mathbb{R},+,\cdot)$	: "	"	"	"
$(\mathbb{C},+,\cdot)$	: "	"	"	"
$(\mathbb{Z}_n,+_n,\cdot_n)$	: "	"	"	"

Note: A ring $(R,+,\cdot)$ supports $+, -$ and $\times$.

Field: A field $(\mathbb{F},+,\cdot)$ is a commutative ring with unit in which all non-zero elements have their inverse with respect to the second operation '$\cdot$'.

i.e. $(\mathbb{F},+,\cdot)$ is called a field if

(1) $(\mathbb{F},+)$ is an abelian group.

(2) $(\mathbb{F},\cdot)$ is a semi group.

(3) $\exists\ 1\in\mathbb{F}$ s.t. $1\cdot a = a\cdot 1 = a \ \forall\, a\in\mathbb{F}$

(4) $\forall\, a(\neq \underset{\substack{\downarrow\\ \text{identity}\\ \text{w.r. to } +}}{0})\in\mathbb{F}\ \exists\ a^{-1}\in\mathbb{F}$ s.t. $a\cdot a^{-1} = a^{-1}\cdot a = 1$.

⑤ '$\cdot$' is distributive over '$+$' i.e.

$\forall\, a, b, c \in \mathbb{F}$, $\quad a\cdot(b+c) = (a\cdot b) + (a\cdot c)$ &

$(a+b)\cdot c = (a\cdot c) + (b\cdot c)$

Note: A field $(\mathbb{F}, +, \cdot)$ supports $+, -, \times$ & $\div$.

Ex:

$(\mathbb{R}, +, \cdot)$: Field
$(\mathbb{Q}, +, \cdot)$: "
$(\mathbb{C}, +, \cdot)$: "

} Infinite Fields

$(\mathbb{Z}, +, \cdot)$: Not a field.

Finite Fields: Fields with finite no. of elements.

Finite fields are also called Galois Fields.

* Galois (French Mathematician) showed that order of finite fields is of the form p^m where p is prime and m is a +ve integer.

i.e. if $(\mathbb{F}, +, \cdot)$ is a finite field then $|\mathbb{F}| = p^m$, p - prime, $m \in \mathbb{N}$

A finite field of p^m is denoted by

$$\underline{GF(p^m)}$$

$m=1$ ← → $m>1$

Prime Fields $(GF(p))$ | Extension Fields $(GF(p^m),\ m>1)$

Ex:

$GF(2)$ $\quad (\{0,1\}, +_2, \cdot_2)$

$GF(p)$ $\quad (\mathbb{Z}_p, +_p, \cdot_p)$ $\quad \mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

p → prime

$GF(2^8) = GF(256)$: AES (Advanced Encryption Std.)

GF(2)

$\{0,1\}, \quad +_2, \quad \cdot_2$

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$e_+ = 0, \qquad e_\circ = 1$

$-a$: Additive inverse of a

a^{-1}: Multiplicative inverse of a.

a	0	1
$-a$	0	1

a	0,	1
a^{-1}	·	1

Remarks : 1. $+_2$ operation on $\{0,1\}$ is same as exclusive-or operation.

2. $\cdot_2$ operation is same as 'AND' operation on two binary digits.

3. Addition & Subtraction operations are same (XOR operation)

4. Mult & division " " " ('AND' ")

Euler's Phi-function: (Euler's Totient function):

$$\phi(n) = |\{ m \in \mathbb{N} \mid m < n \ \& \ \gcd(m,n) = 1 \}|$$

= No. of +ve integers less than n & coprime to n.

$= |\mathbb{Z}_n^*|$

Properties:
1. $\phi(1) = 0$
2. $\phi(p) = p-1$, p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$, where m & n are coprime.
4. $\phi(p^e) = p^e - p^{e-1}$, p is prime.

5. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ ($p_1, p_2, \ldots, p_k$ are primes)

$$\phi(n) = \phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdot \phi(p_3^{e_3}) \cdots \phi(p_k^{e_k})$$

$$= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

$$= \underbrace{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\boxed{\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)}$$

Fermat's Little Theorem

First version: If p is a prime number and a an integer such that p doesn't divides a then

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

Second version: If p is prime and a is an integer then

$$\boxed{a^p \equiv a \bmod p}$$

Euler's Theorem

First version: If a & n are coprime then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Second version: If $n = p \times q$, $a < n$ and k is an integer then

$$\boxed{a^{k \times \phi(n) + 1} \equiv a \pmod{n}}$$

RSA cryptosystem use Euler's theorem.