**Elliptic Curve Cryptography (Additional Points)**

-------------------------------------------------------------------------------------------------------------------------------------------------

1) Using a group of points (instead of integers) for cryptographic schemes 🡪 Reducing Computational Loads

2) For each point on the curve: and

Notice: is the infinity point.

3) **Finite Field (a.k.a. Galois Field)**

* Containing a Finite Number of Elements
* The operations of Multiplication, Addition, Subtraction, and Division are defined in a finite field.
* Order = The number of elements of a finite field.
* Symbol = GF(?) or
* There are two common types of finite fields:
* Prime Field: 🡪 Size = Number of bits of .
* Binary Field: 🡪 Size = Number of bits of .
* Prime Field Elliptic Curve Equation:
* Binary Field Elliptic Curve Equation:
* Every element in a binary field can be presented as a polynomial:
* In this context, an irreducible polynomial is defined: 🡪 **Mod** Polynomial for Operations
* Binary Field Equation:
* Three main operations in binary field with mode 🡪 Addition, Multiplication, and Inversion
* Addition:
* Multiplication:
* Inversion:

Binary Field Example:

Notice: In prime field, should be greater than three 🡪

Rule 1: Adding “P” copies of any element in a finite field of order “P” results in getting 0.

Rule 2: The outcome of performing an operation on any two elements of a finite field should exist in that field.

4) **Modular Operations** 🡪 Providing this possibility to have all of the data points and results on the curve.

5) Subtraction and Division Operations 🡪 They are defined in terms of addition and multiplication operations.

6) Inversion Operation 🡪 It is required for implementing division operation.

7) **Point Addition and Point Doubling**

* Elliptic Curve (E):
* Considering two data points on the curve: and
* Result Data Point 🡪 🡪 and , both in mod
* Point Doubling Equations:
* Point Addition Equations: