Presentation Topic: **Finite Fields**

Course Title: Advanced Cryptography

Course Code: ICT-6115

Presented by :

Rejaul Hasan Rasel
IT-23609
Dept. of ICT,
MBSTU

Supervised By:

Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,
MBSTU

Outline

- Structure of a Finite Field
- Properties and Examples
- Polynomial Codes and Their Importance
- Applications in Coding Theory
- Summary and Conclusion

Objectives

- Understand the structure and properties of finite fields.
- Learn how polynomial codes are constructed and their significance in error correction.
- Explore applications of these concepts in real-world scenarios.

Structure of a Finite Field

Definition:

- A finite field (or Galois field) is a field with a finite number of elements.
- Denoted as GF(p^n), where p is a prime, and n is a positive integer.

Properties:

- The number of elements in GF(p^n) is p^n.
- Field addition and multiplication follow modulo p arithmetic.
- Multiplicative inverses exist for all nonzero elements.

Examples:

- GF(2): Binary field with elements {0, 1}.
- GF(4): Field with 4 elements, defined by a polynomial over GF(2).

Polynomial Codes

What are Polynomial Codes?

- Error-detecting and error-correcting codes based on polynomials over finite fields.
- Includes linear codes like BCH codes, Reed-Solomon codes, etc.

Key Concepts:

- Codewords are derived from polynomial evaluations in GF(p^n).
- Encoding and decoding depend on polynomial division and modular arithmetic.

Example:

- Reed-Solomon codes used in data storage and communication systems.

Applications

Finite Fields:

- Cryptography (e.g., RSA, Elliptic Curve Cryptography).
- Pseudorandom number generation.
- Algebraic geometry and number theory.

Polynomial Codes:

- Data integrity in storage devices (e.g., CDs, DVDs, RAID systems).
- Reliable communication (e.g., satellite and wireless communication).
- QR codes and barcodes.

Conclusion

- Finite fields provide the foundation for modern coding theory and cryptography.
- Polynomial codes are indispensable for ensuring data reliability and error correction.
- Applications demonstrate the practical significance of abstract algebra in technology.

References

- Judson, Thomas W. Abstract Algebra: Theory and Applications.
- Additional resources: [Your list of references].