CS641

Modern Cryptology

Lecture 8

FIELDS

INFORMAL DEFINITION

A set of numbers on which full arithmetic can be done.

- Set of rational numbers ($\mathbb{Q}$), real numbers ($\mathbb{R}$), complex numbers ($\mathbb{C}$) are fields as they admit all four arithmetic operations: $+$, $-$, $*$, and $/$.
- Set of integers ($\mathbb{Z}$) is not a field as division is not always possible.

Non-standard Fields

- Consider $F_2 = \{0, 1\}$ with addition and multiplication modulo 2.
- Subtraction is same as addition, and division is trivial.
- Is it a field?
- We need to formally define notion of numbers and arithmetic operations to properly identify fields.

Groups

Definition

A set of elements G with binary operation $\cdot$ defined on elements such that:

1. $a \cdot b \in G$ for any $a, b \in G$ [closure]
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in G$ [associativity]
3. There exists $e \in G$ such that $a \cdot e = e \cdot a = a$ for any $a \in G$ [identity]
4. There exists $b \in G$ such that $a \cdot b = e$ for any $a \in G$ [inverse]

- Groups capture properties of $+$ and $*$ operations in a field.
  - $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$ are groups
  - $(\mathbb{Q} \setminus \{0\}, *)$, $(\mathbb{R} \setminus \{0\}, *)$, and $(\mathbb{C} \setminus \{0\}, *)$ are groups but $(\mathbb{Z} \setminus \{0\}, *)$ is not.

Commutative Groups

Definition

A group $(G, \cdot)$ with following additional property: $a \cdot b = b \cdot a$ for any $a, b \in G$ [commutativity]

- Example groups of last slide are all commutative.
- Not all groups are commutative though:
  - $(GL_n(\mathbb{Q}), \cdot)$ is a non-commutative group of all $n \times n$ invertible matrices with rational entries under multiplication.
  - $(S_n, \circ)$ is a non-commutative group of all permutations of $[1, n]$ under composition.

Rings

Definition

A set of elements R with two binary operations $+$ and $*$ defined on elements such that:

1. $(R, +)$ is a commutative group.
2. $(R \backslash \{0\}, *)$ satisfies closure, associativity, and identity properties.
3. $a * (b + c) = a * b + a * c$ for any $a, b, c \in R$ [distributivity]

- Rings capture arithmetic without division:
  - $(\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$, $(\mathbb{C}, +, *)$, $(\mathbb{Z}, +, *)$ are rings.
- $(R, +, *)$ is commutative ring if multiplication operation is also commutative:
  - $(M_n(\mathbb{Q}), +, \cdot)$ is a non-commutative ring where $M_n(\mathbb{Q})$ is set of $n \times n$ matrices with rational entries.

Fields

Definition

A set of elements F with two binary operations $+$ and $*$ defined on elements such that:

1. $(F, +)$ is a commutative group.
2. $(F \backslash \{0\}, *)$ is a commutative group.
3. $a * (b + c) = a * b + a * c$ for any $a, b, c \in F$ [distributivity]

- Fields are commutative rings that admit division:
  - $(\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$, and $(\mathbb{C}, +, *)$ are fields but $(\mathbb{Z}, +, *)$ is not.
- The set of non-zero elements of F is represented as F^*.

Prime Fields

- Let $F_p = \{0, 1, \ldots, p-1\}$ for a prime p.
- Then, $(F_p, +, *)$ is a field where arithmetic is modulo p:
  - $(F_p, +)$ is a commutative group with (additive) inverse of $a \in F_p$ being $p - a$ for $a \neq 0$.
  - $(F_p^*, *)$ is a commutative group with (multiplicative) inverse of $a \in F_p^*$ being $b \in F_p$ where $ab + rp = 1$.

Function Fields

- Let $F[x]$ be the set of all polynomials in x with coefficients from field F.
- Then, $(F[x], +, *)$ is a commutative ring where arithmetic is over polynomials.
- Let $F(x)$ be the set of rational functions in x, that is:

$$F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \right\}.$$

- Then, $(F(x), +, *)$ is a field:
  - Multiplicative inverse of f/g, $f \neq 0$, is g/f.
  - All other properties can be readily verified.

Prime Extension Fields

- Let $f(x) \in F_p[x]$ be an irreducible polynomial over F_p.
  - $f(x)$ cannot be factored as $f_1(x)f_2(x)$ with $f_1, f_2 \in F_p[x]$, both of degree > 0.
- Let degree of f be d.
- Define F_{p^d} to be set of all polynomials of degree $< d$ in $F_p[x]$.
- Then, $(F_{p^d}, +, *)$ is a field with arithmetic modulo p and $f(x)$:
  - All coefficients are reduced modulo p and all powers of x of degree $\geq d$ are reduced modulo $f(x)$.
  - Multiplicative inverse of $g \in F^*_{p^d}$ is $h \in F_{p^d}$ such that $gh + rf = 1$ modulo p.
  - Remaining properties are straightforward.

Finite Fields

$(F, +, *)$ is a finite field if $|F|$ is finite.

- Fields F_{p^d} for $d \geq 1$ and prime p are examples of finite fields.

Theorem

1. A finite field has size p^d where p is a prime and $d \geq 1$.
2. There is only one field of size p^d, namely, F_{p^d}.

Finite Fields: Usefulness

- In cryptography, we often do arithmetic over input plaintext to produce ciphertext.
- Arithmetic operations over natural fields ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$) change the size: addition may add one bit and multiplication may double the bit size.
- This is undesirable as we would prefer to have ciphertext of the similar size as plaintext.
- Therefore, we work over F_{p^d} for suitably chosen prime p and $d \geq 1$.
- All numbers in F_{p^d} have the same size—in particular, numbers in F_{2^d} require d bits.

Key Properties of Finite Groups

Order

Let $(G, \cdot)$ be a finite commutative group, and $a \in G$. Order of a is the smallest non-zero number k such that $a^k = e$.

Lemma

Order is well-defined for every element of a finite commutative group.

- Let $a \in G$.
- Consider the set $A = \{a^i \mid i > 0\} \subseteq G$.
- Since G is finite, A is finite too.
- Let a^k be the largest power of a in A.
- Then $a^{k+1} = a^i$ for some $i \leq k$.
- This gives $a^{k+1-i} = e$ showing that order of a is well-defined.

Key Properties of Finite Groups

Lemma

If order of a equals k, then for every ℓ such that $a^\ell = e$: $k \mid \ell$.

- Let $m = \gcd(k, \ell) = uk + v\ell$ for some $u, v \in \mathbb{Z}$.
- Then $a^m = a^{uk+v\ell} = (a^k)^u \cdot (a^\ell)^v = e$.
- By definition of order, $k \leq m$.
- Since $m \mid k$, $m = k$ showing $k \mid \ell$.

Key Properties of Finite Groups

Theorem

Let $(G, \cdot)$ be a finite commutative group. Then for every $a \in G$: $a^{|G|} = e$.

- Let $m = |G|$ and $b_1, \ldots, b_m$ be all elements of G.
- Consider the sequence of elements $ab_1, ab_2, \ldots, ab_m$.
- Each is in G and distinct:
  - If $ab_i = ab_j$ then $b_i = b_j$.
- Therefore, $\prod_{i=1}^{m} b_i = \prod_{i=1}^{m} ab_i = a^m \prod_{i=1}^{m} b_i$.
- This shows $a^m = e$.

Corollary

For a finite group of size m, order of every element divides m.

Key Properties of Finite Groups

Cyclic Groups

Let $(G, \cdot)$ be a commutative group. G is cyclic if there exists $a \in G$ such that $G = \{a^i \mid i \in \mathbb{Z}\}$. Element a is called generator of the group. If G is finite, then order a equals $|G|$.

- $(\mathbb{Z}, +)$ is a cyclic group with generator 1.
- $(F_p, +)$ is a cyclic group with generator 1, and order of 1 is p.
- $(\mathbb{Q}, +)$ is not a cyclic group.
- $(F_{p^d}, +)$ is not a cyclic group for $d > 1$.

Key Properties of Finite Fields

Theorem

For a finite field F, $(F^*, *)$ is a cyclic group.

- Let $m = |F^*|$ and $m = \prod_{i=1}^{t} p_i^{r_i}$ where p_i are prime numbers and $r_i \geq 1$.
- Let $S_i = \{a \mid a \in F^* \text{ and order of } a \text{ divides } p_i^{r_i}\}$.
- S_i is also a group.
- S_i is a cyclic group:
  - Let $a_i \in S_i$ be an element with maximum order $p_i^{s_i}$, for some $s_i \leq r_i$.
  - Order of every element of S_i will divide $p_i^{s_i}$.
  - Therefore, every element of S_i satisfies the equation $y^{p_i^{s_i}} = 1$.
  - By field property, $|S_i| \leq p_i^{s_i}$.
  - Since a_i has $p_i^{s_i}$ distinct powers, all in S_i, a_i is generator of S_i.

Key Properties of Finite Fields

- By Structure Theorem of Finite Commutative Groups, any element of F^* can be uniquely written as a product of one element of S_i for each i.
- Therefore, $m = \prod_{i=1}^{t} p_i^{s_i}$.
- This forces $s_i = r_i$ for every i.
- Let $a = \prod_{i=1}^{t} a_i$.
- a is a generator of F^*:
  - Let $a^{m'} = 1$.
  - Then $1 = a^{m'} = \prod_{i=1}^{t} a_i^{m'}$.
  - Above Structure Theorem forces $a_i^{m'} = 1$ for every i.
  - Therefore, $p_i^{r_i} \mid m'$ implying $m \mid m'$.

Key Properties of Finite Fields

Theorem

Let F be any finite field. Then polynomial $q(y) \in F[y]$ of degree d has at most d roots in F.

- Proof is by induction on d.
- For $d = 1$, $q(y) = ay + b$ and so has at most one root ($= b/a$) if $a \neq 0$.
- Assume for $d - 1$, and consider $q(y)$ of degree d.
- Let $a \in F$ be a root of $q(y)$, that is, $q(a) = 0$.
- Then, $q(y) = q(y) - q(a) = (y - a) \cdot q'(y)$ where $q'(y)$ has degree $d - 1$.
- Let $b \in F$ be another root of $q(y)$, $b \neq a$.
- Then $0 = q(b) = (b - a) \cdot q'(b)$.
- This implies $q'(b) = 0$.
- By induction hypothesis, there are at most $d - 1$ roots of $q'(y)$ in F.
- So there are at most d roots of $q(y)$ in F.