18733: Applied Cryptography Recitation

Algebraic Structures and Number Theory

Gihyuk Ko

March 3, 2017

Carnegie Mellon University

Why Number Theory?

Cryptographers know what they want before they take it

- I want a public key crypto system
- I want one-way functions
- I want a PRG

Number theory has provided very elegant solutions to many questions in cryptography

Sets of elements with operation and structure

- ex) Set of all integers with addition
- ex) All integers mod 10 with addition mod 10
- ex) All invertible nxn matrices with matrix multiplication
- ex) All nonzero real numbers with multiplication

Groups

A group is a set **G** with some operation $\cdot$ that has the following properties:

- $\forall a, b \in G, a \cdot b \in G$ **(Closure)**
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. $\forall a, b, c \in G$ **(Associative)**
- $\exists 1 \in G$. $1 \cdot a = a$ and $a \cdot 1 = a$. $\forall a \in G$ **(Identity)**
- $\forall a \in G$. $\exists b$ s.t. $a \cdot b = 1$ and $b \cdot a = 1$ **(Inverse)**

If a group G is also commutative, G is called an *Abelian Group*

The *order* of a group G: $|G|$

If $|G|$ is finite, then G is a *finite group*

Groups: Examples

- $(\mathbb{Z}, +)$: Set of integers under addition
- $(\mathbb{R}, +)$: Set of real numbers under addition
- $(\mathbb{R}/\{0\}, \times)$: Set of non-zero real numbers under multiplication
- $(\mathbb{Z}_n, +)$: Set of positive integers under addition mod n
- $(GL_n, \times_n)$: General linear group (set of all $n \times n$ invertible matrices)
- $(\mathbb{Z}/\{0\}, \times)$: Set of all non-zero integers under multiplication

Rings

A ring is a set **R** with two operations $(+, \cdot)$ that has the following properties:

- R is an *Abelian group* under $+$
- $\forall a, b \in R, a \cdot b \in R$ **(Closure)**
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall a, b, c \in R$ **(Associative)**
- $a \cdot b = b \cdot a.\ \forall a, b \in R$ **(Communitive)**
- $\exists 1 \in R$ s.t. $1 \cdot a = a$ and $a \cdot 1 = a.\ \forall a \in R$ **(Identity)**
- $a \cdot b + c = a \cdot b + a \cdot c.\ \forall a, b, c \in R$ **(Distributive)**

Rings: Example

$(\mathbb{Z}_n, +, \times)$: Integers modulo n under addition and multiplication

ex) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Group under addition

Closed under multiplication

Associative and communitive under multiplication

Identity is 1

Distributive

Fields

A field is a set **F** with two operations $(+, \cdot)$ that has the following properties:

- F is an *Abelian group* under $+$
- The non-zero elements of F are an *Abelian group* under $\cdot$
- $a \cdot (b + c) = a \cdot b + a \cdot c.\ \forall a, b, c \in F$ (Distributive)

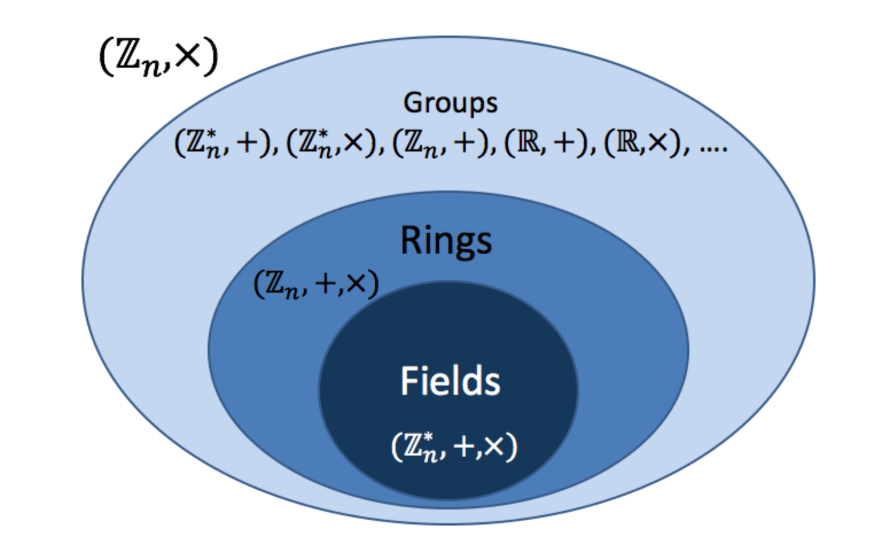
A field is a ring with multiplicative inverses

Notes

Consider a set $\mathbb{Z}_n$ and operation $\times$

- $a \in \mathbb{Z}_n$ has an inverse iff $gcd(a, n) = 1$
    - Proof in class notes
- Form a group from $\mathbb{Z}_n$ by taking the elements for which an inverse exists
- Call this $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | gcd(a, n) = 1\}$

    Mini-homework: Show that $\mathbb{Z}_n^*$ is a group for every n!
- $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ if p is prime


$(\mathbb{Z}_n,\times)$
Groups
$(\mathbb{Z}_n^*,+), (\mathbb{Z}_n^*,\times), (\mathbb{Z}_n,+), (\mathbb{R},+), (\mathbb{R},\times)$, ...
Rings
$(\mathbb{Z}_n,+,\times)$
Fields
$(\mathbb{Z}_n^*,+,\times)$

Subgroups

Let G be a group

- $S \nsubseteq G$, if S is also a group, we call S a subgroup of G
- ex) Take G, and form S by taking the identity element 1 and another element say g, so $S = \{1, g\}$, then expand S by taking the closure under the group operation
    - $S = \{1, g, g^2, g^3, ...\}$
    - $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is a subgroup of $\mathbb{Z}$

Subgroups (cnt'd)

- **Lagrange's Theorem**: Let H be a subgroup of a finite group G. The order of H divides the order of G.
- *Corollary*: If $|G|$ is prime, then $|H|$ is either $|G|$ or 1.
- Implication: Not always easy to find a generator of a group, so instead find groups of prime order, i.e. $|G| = p$, then every element other than 1 is a generator.

Quadratic Residue Subgroup

Given a group $(\mathbb{Z}_n^*, \times)$

- Quadratic Residue Subgroup of $\mathbb{Z}_n^*$: $\mathbf{QR_n^*} = \{x^2 \in \mathbb{Z}_n^* | x \in \mathbb{Z}_n^*\}$
- The set of all elements that are the result of squaring some other element in the group
- This group is important anytime we want to compute square roots, we need to know that the square root for each element in the group will exist

Useful facts:

- Given p an odd prime, $x^2 = 1 \pmod{p}$ has two solutions: $x = 1 \pmod{p}$ or $x = -1 \pmod{p}$.
- *Fermat's Theorem*: $x^{(p-1)} = 1 \pmod{p}$, where $p - 1$ is an even number
- $|QR_p^*| = |Z_p^*|/2$

Legendre and Jacobi Symbol

Given a group $(\mathbb{Z}_p^*, \times)$ where $p > 2$ is a prime

- Legendre Symbol $\mathbf{L_p(x)} = x^{\frac{(p-1)}{2}} \pmod{p}$
- $L_p(x) = 1 \Rightarrow x \in QR_p^*$
- $L_p(x) = -1 \Rightarrow x \notin QR_p^*$

Given a group $(\mathbb{Z}_n^*, \times)$ where $n = \prod_i p_i^{c_i}$ is a prime factorization of n

- Jacobi Symbol $\mathbf{J_n(x)} = \prod_i L_{p_i}(x)^{c_i} \pmod{n}$

Miller-Rabin Primality Test

Fermat's Theorem: If p is an odd prime, $a^{p-1} = 1 \bmod p$ for all a

A quick reject test: if $a^{p-1} \bmod p \neq 1 \bmod p$: reject!

Miller-Rabin test: if $a^{p-1} \bmod p = 1 \bmod p$:

- Let $p - 1 = c \cdot 2^b$ where c: odd number, $b > 0$

$$a^{p-1} \bmod p = [\ldots[a^c \bmod p]^2 \ldots]^2 \bmod p$$

- **Fact**:
    - If p is an odd prime, then $a^c = 1 \bmod p$ or $a^{c \cdot 2^r} = -1 \bmod p$ for some r
- Test(a): check if $a^c = 1 \bmod p$ or $a^{c \cdot 2^r} = -1 \bmod p$, `accept` if yes, `reject` if no.
- Repeat Test(a) for multiple values of a, `accept` if every test passes.

Discrete Logarithm and Legendre Symbol

Theorem: Let p be a prime, g a generator of Z_p^*, and $p-1 = c \cdot 2^b$. Given $y = g^x \bmod p$, There exists an efficient algorithm which computes b least significant bits of x

- `Step 1`: Calculate Legendre symbol of y as $L_p(y) = y^{\frac{p-1}{2}} \bmod p$
- `Step 2a`: If $L_p(y) = 1$ then $y \in QR_p^* \to 2 \mid x, lsb(x) = 0$. goto `Step 3a`.
- `Step 2b`: If $L_p(y) = -1$ then $y \notin QR_p^* \to 2 \nmid x, lsb(x) = 1$. goto `Step 3b`.
- `Step 3a`: Set $y' = \sqrt{y} \bmod p = g^{\frac{x}{2}} \bmod p$, goto `Step 1`.
- `Step 3b`: Set $y' = \sqrt{y \cdot g^{-1}} \bmod p = g^{\frac{x-1}{2}} \bmod p$, goto `Step 1`.

  Repeat above procedure for b times, and we get b-bit lsb of x! $\square$

Questions?