Implementation Security In Cryptography

Lecture 06: Finite Field and Hardware

Recap

- In the last lecture
  - Basics of Hardware Design

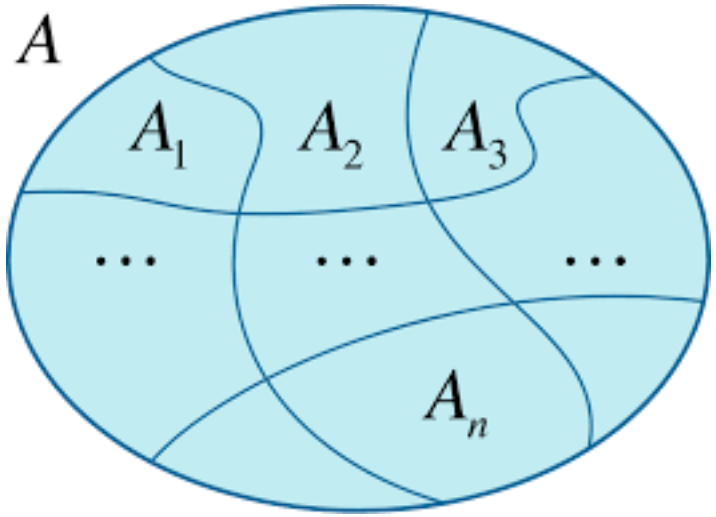
Today

- Finite Field — Mathematics and Hardware

Congruences

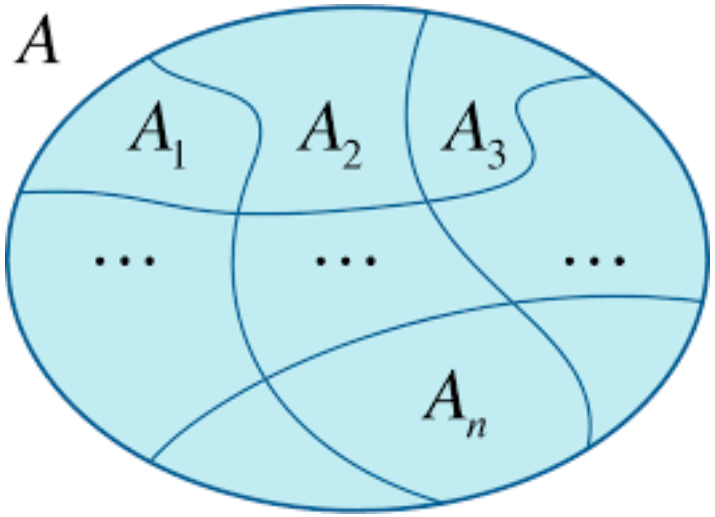
- What is $a \equiv b \ mod \ n$?

Congruences



- What is $a \equiv b \ mod \ n$?
  - $n \mid (b - a)$
- This is an equivalence relation
  - $a \equiv a \ mod \ n$ — reflexive
  - $a \equiv b \ mod \ n \implies b \equiv a \ mod \ n$ — symmetric
  - $a \equiv b \ mod \ n \wedge b \equiv c \ mod \ n \implies a \equiv c \ mod \ n$ — transitive
  - Therefore, this relation will create disjoint partitions over the set of integers.

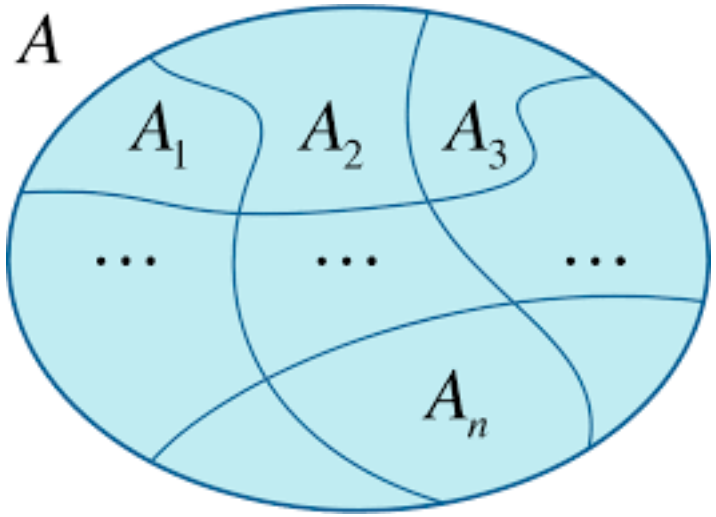
Residue Class



- $a \equiv b \ mod \ n$
  - $n \mid (b - a)$
  - $a = b + kn, k \in \mathbb{Z}$
  - The equivalent classes are as follows:
    - $a \ mod \ n$ consists of all integers that are obtain by adding (subtracting) kn with a.
  - Example: Let say n = 7
    - Residue class $1 \ mod \ 7 = \{1, 1 \pm 7, 1 \pm 2 * 7, \cdots\}$

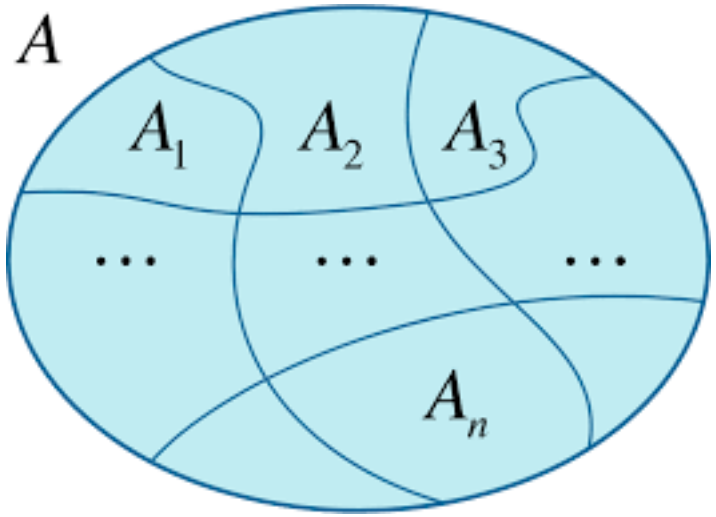
Residue Class

- Set of all residue classes mod n
  - Denoted as Z/nZ
  - How many elements does this set have?



Residue Class

- Set of all residue classes mod n
  - Denoted as Z/nZ
  - How many elements does this set have?
    - [0], [1], [2] ,…, [n-1]
  - Now let’s talk only in terms of these classes..



Some Important Theorems

- $a \equiv b \ mod \ n$, and $c \equiv d \ mod \ n$ implies
  - $-a \equiv -b \ mod \ n$
  - $a + c \equiv b + d \ mod \ n$
  - $ac \equiv bd \ mod \ n$
- Try the proofs by yourself

Group

- A group is a mathematical structure with a (nonempty) set and a (binary) operator $(G, +)$.
  - **Closure**: $a, b \in G \implies a + b \in G$
  - **Associativity**: $a, b, c \in G \implies a + (b + c) = (a + b) + c$
  - **Identity**: $\exists e \in G, \forall a \in G, a + e = e + a = a$
  - **Inverse**: $\forall a \in G, \exists a^{-1} \in G, a + a^{-1} = a^{-1} + a = e$
- A group is *abelian* or *commutative* if $\forall a, b \in G, a + b = b + a$

Examples

- The set of integers with +
  - The sums are also integers
  - a+(b+c) = (a+b)+c
  - 0 is the identity element
  - -a is the inverse of a.
- Does the set of integers form a group under multiplication?
- Set of rational numbers under multiplication?

What About the Residue Classes

- The set of residue classes form a group under “addition”
  - The addition is between classes: [a] + [b]
    - => a mod n + b mod n = (a + b) mod n
  - It is closed
  - It is associative
  - [0] is the identity
  - Inverse of [a] is basically [n - a]

$(\mathbb{Z}_3, +_3)$	$[\![0]\!]_3$	$[\![1]\!]_3$	$[\![2]\!]_3$
$[\![0]\!]_3$	$[\![0]\!]_3$	$[\![1]\!]_3$	$[\![2]\!]_3$
$[\![1]\!]_3$	$[\![1]\!]_3$	$[\![2]\!]_3$	$[\![0]\!]_0$
$[\![2]\!]_3$	$[\![2]\!]_3$	$[\![0]\!]_3$	$[\![1]\!]_3$

What About the Residue Classes

- The set of residue classes form a group under “addition”
  - The addition is between classes: [a] + [b]
    - => a mod n + b mod n = (a + b) mod n
  - It is closed
  - It is associative
  - [0] is the identity
  - Inverse of [a] is basically [n - a]
- The set of residue classes is also a group under multiplication **under certain conditions**

$(\mathbb{Z}_3, +_3)$	$[\![0]\!]_3$	$[\![1]\!]_3$	$[\![2]\!]_3$
$[\![0]\!]_3$	$[\![0]\!]_3$	$[\![1]\!]_3$	$[\![2]\!]_3$
$[\![1]\!]_3$	$[\![1]\!]_3$	$[\![2]\!]_3$	$[\![0]\!]_0$
$[\![2]\!]_3$	$[\![2]\!]_3$	$[\![0]\!]_3$	$[\![1]\!]_3$

Multiplicative Group Module n

- We denote it by $((\mathbb{Z}/\ n\mathbb{Z}, \circ)$ or $((\mathbb{Z}_n, \circ)$
  - The addition is between classes: [a] * [b]
    - => (a mod n) * (b mod n) = (a + k1*n)(b + k2*n) = ab + a*k2*n + b*k1*n + k1*k2*n^2 = ab + (a*k2 + b*k1 + k1*k2*n)*n = ab + k3*n = [ab]
  - It is closed
  - It is associative (prove it)
  - [1] is the identity
  - But where is the inverse?????
- **Turns out that inverse only exist for certain elements not for all**
- **Let's define this subset as $\mathbb{Z}_n^*$ — this indeed forms a group**

Multiplicative Group Module n

- What are the elements of $\mathbb{Z}_n^*$?

Multiplicative Group Module n

- What are the elements of $\mathbb{Z}_n^*$?
  - Elements that are co-prime to n
  - Another way: gcd(a,n) = 1
- What happens if n is a prime, say p?

Multiplicative Group Module n

- What are the elements of $\mathbb{Z}_n^*$?
  - Elements that are co-prime to n
  - Another way: gcd(a,n) = 1
- What happens if n is a prime, say p?
- $|\mathbb{Z}_n^*| = p - 1$
- How many elements in $\mathbb{Z}_n^*$ can be there if n is not a prime?
  - This number is called $\Phi(n)$ — **Euler's Totient Function**
  - **Example:** $\Phi(26) = 13$**,** $\Phi(p) = p - 1$**, if p is prime**

Fermat's Little Theorem

- If gcd(a, n) = 1, then $a^{\Phi(n)} = 1 \ mod \ n$
  - That means for any element of $\mathbb{Z}_n^*$, we can raise it to the power of $\Phi(n)$ and end up in the identity element!!!
- Proof: Will not be discussed for the sake of time!! I can tell you later if you are interested..
- $a^{p-1} = 1 \ mod \ p$, if p is prime.
- Interesting fact: $a^{p-2} = a^{-1} \ mod \ p$

Small Examples

- Let's consider $\mathbb{Z}_4^*$
- What are the elements? [1], [3] — let's abuse the notation and denote as 1, 3
- $\Phi(4) = 2$
- So, let's see $3^4 \ mod \ 4$ = 81 mod 4 = 1 !!!
- Calculate: $2^{1000} \ mod \ 13$ = $2^{(83\times12)+4} \ mod \ 13 = 16 \ mod \ 13 = 3 \ mod \ 13$

Ring

- Let's consider a (nonempty) set with two operations $(G, +, \circ)$
  - G is an abelian group under addition
  - G is closed under multiplication
  - Multiplication is associative
  - There is an identity element
  - **But not every element has a multiplicative inverse (other than 0)**.
  - Also, multiplication is **distributive** on addition
    - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity).
    - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity)
  - If the multiplication is commutative we call it **commutative ring**

Example

- Consider $\mathbb{Z}_n$ with + and ∘
  - G is a ring if n is composite, there is no inverse unless gcd(a,n) = 1.
- Consider $\mathbb{Z}_4$ — 2 does not have an inverse — no element can be multiplied with 2 giving 1. Rather 2*2 mods 4 = 0. 2 is, therefore, called a **zero divisor**.
- But then consider $\mathbb{Z}_5$ — It is also a ring, but you can see that every element has an inverse.

Field

- Let's consider a (nonempty) set with two operations $(G, +, \circ)$
  - G is commutative ring with every element except 0 having a multiplicative inverse.
- Example:
  - Set of real numbers with addition and multiplication
  - Set of rational numbers with addition and multiplication
  - Set of complex numbers with addition and multiplication
  - **Set of integers modulo a prime**