# Week 3



Lecture 2

Properties of Numbers III

Udaya Parampalli



School of Computing and Information Systems
University of Melbourne



THE UNIVERSITY OF MELBOURNE

Lecture 1
Modern Symmetric key Ciphers



**Lecture 2**
**Properties of Numbers III**



Workshop 3: Workshops based on Lectures in Week 2

Quizz 3

- Numbers, Divisibility, Mod Operation, GCD, Extended GCD
- Inverse Mod n
- Properties Euler's Phi ($\phi$) Function
- $\phi(p) = p - 1$, for any prime $p$.
- $\phi(p^a) = p^{a-1}(p-1)$, for any prime $p$ and any integer $a \geq 1$.
- $\phi(pq) = (p-1)(q-1)$, for any two primes $p$ and $q$.
- In fact, $\phi(mn) = \phi(m)\phi(n)$, for any two numbers which are relatively prime.

let $\mathbf{Z}_n^\star$ be set of numbers from 1 to $n-1$ but are relatively prime.

**Theorem**

*If $a \in \mathbf{Z}_n^\star$, then $a^{\phi(n)} = 1 \pmod{n}$.*

# Inverse Mod n

**Using Extended GCD Algorithm**

*Function*$(a, n)$

g,x,y:=XGCD(a,n);

If g eq 1 then Return(x)

else Return("The Inverse Does not Exist"), end if;

*end function*;

**Using Eulerś Phi Function Result**

*Function*$(a, n)$

$inva := a^{\phi(n)-1} \pmod{n}$.

*Return*$(inva)$;

*end function*;

The later function works only if $a$ is relatively prime to $n$.

**Definition**

*Remainders mod n: For $n \geq 1$, the set of remainders obtained by dividing integers by n, precisely these are elements of $\mathbf{Z}_n = \{0, 1, \cdots, n-1\}$.*



However, not all elements of $\mathbf{Z}_n$ can be inverted. We define further the set of invertible numbers in $\mathbf{Z}_n$.



**Definition**

*Reduced set of residues mod n: For $n \geq 1$, the reduced set of residues, R(n) is defined as set of residues modulo n which are relatively prime to n.*



Sometimes, $R(n)$ is also represented as $\mathbf{Z}^\star(n)$. In fact $\phi(n) = \#R(n)$, the cardinality(size) of the set $R(n)$.
Example: $\phi(15) = 8$, because $\phi(15) = \phi(5 \times 3) = (4 \times 2) = 8$.
$\phi(37) = 36$, as 37 is a prime number.
Next we consider Euler's theorem.

**Theorem**

*If $a \in \mathbf{Z}_n^\star$, then $a^{\phi(n)} = 1 \pmod{n}$.*



Proof: Let $R(n) = \{r_1, r_2, \ldots, r_{\phi(n)}\}$, be reduced set of residues modulo $n$. Now consider the set $a\ R(n) = \{a\ r_1, a\ r_2, \ldots, a\ r_{\phi(n)}\}$. Since $a$ is relatively prime to $n$, the set $aR(n)$ is identically equal to $R(n)$. Note that the process of multiplying $a$ only rearranges the residues in $R(n)$. Hence we can multiply all the elements in $R(n)$ and equate with the multiplication of all the elements of $a\ R(n)$. Hence we can write:



$$r_1 \times r_2 \cdots \times r_{\phi(n)} = (ar_1) \times (ar_2) \cdots \times (ar_{\phi(n)}).$$



Note that $r_i$s are relatively prime to $n$ and hence we can cancel $r_i$ in the above equation by multiplying $r_i^{-1}$, $i = 1 \cdots \phi(n)$, to both the side of the equation. Then the above equation simplifies to

$$1 = a^{\phi(n)}. \text{ Hence the result.}$$

# Euler's Theorem example when $n = pq$



When $n = pq$, $p$ and $q$ are primes, then $\phi(n) = (p-1)(q-1)$.

**Theorem**

*If $a \in \mathbf{Z}^{\star}_{pq}$, then $a^{(p-1)(q-1)} = 1 \pmod{pq}$.*



The above result will be used in next week lectures.

Example: $n = 35$, $\phi(35) = 24$, because

$\phi(35) = (\phi(7) \times \phi(5)) = (6 \times 4) = 24$.



2 is relatively prime to 35

$2^{24} \mod 35 = 1$

**Theorem**

*Let $p$ be a prime number, then if $\gcd(a, p) = 1$, then*

$$a^{p-1} = 1 \ (mod \ p).$$



This is the particular case of Euler's Theorem when $n$ is prime.



**Fermat's Little Theorem**

**Theorem**

*Let $p$ be a prime number,*

$$a^p = a \ (mod \ p), \ \textit{for any integer } a.$$



When $a$ is relatively prime, the theorem follows from the Fermatss theorem. When $a$ is multiple of $p$, the result is trivially true.

- When $p$ is a prime number, we learn that all nonzero numbers less than $p$ are relatively prime and hence they are closed modulo $p$.



- In otherwords, all nonzero elements are invertible in $\mathbf{Z}_p$.
- They are closed under addition modulo $p$.
- Hence $\mathbf{Z}_p$ is closed under addition and multipliaction mod $p$ .



- In fact, $\mathbf{Z}_p$ is a finite field, a structure extensively used in Cryptography.

Let us visit a few concepts that we have learnt already. A *Group* is a set $G$ together with a binary operation $\cdot$ on $G$ such that the following three properties hold:



- $\cdot$ is *associative*; that is, for any $a, b, c \in G$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
- There is an *identity* element $e$ in $G$ such that for all $a \in G$,

$$a \cdot e = e \cdot a = a$$
- For each $a \in G$, there exists an *inverse* element $a^{(-1)} \in G$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$
- If the group also satisfies
For all $a, b \in G$,
$$a \cdot b = b \cdot a$$
then the group is called *abelian* (or *commutative*).

A *Ring* $(R, +, \cdot)$ is a set $R$,together with two binary operations, denoted by $+$ and $\cdot$, such that:



- $R$ is an abelian group with respect to $+$.
- $\cdot$ is associative; that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
- The *distributive laws* hold; that is , for all $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$

# Prime Fields



We note that the set $\mathbf{Z}_p = \{0, 1, \cdots, p-1\}$, where $p$ is a prime number, satisfies axioms of a field.

- The set is closed under addition.
- Since $p$ is prime number, any nonzero element in $\mathbf{Z}_p$ has an inverse (Use Extended Euclidean algorithm).
- you can verify that additions and multiplications are distributive.



In $\mathbf{Z}_p$, unlike in Integers, $p$ times any element in the field is zero in the field. This leads to a concept called "characteristic" of a field. We also denote $\mathbf{Z}_p^\star$ as a set of non-zero elements of $\mathbf{Z}_p$.

**Definition**

*Let $F$ be a field with the multiplicative identity 1 and the additive identity 0. The characteristic of $F$, sometimes written as $char(F)$, is the smallest integer $n \geq 0$ such that addition of the 1 with itself $n$ times results in 0. i.e $n(1) = 0$.*



Note that for real and complex fields you cannot find a positive integer $n$ satisfying the above criteria. Hence, the characteristic of real and complex fields is 0.



In contrast for residue class rings $\mathbf{Z}_n$, the characteristic is $n$. When $n$ is prime, $\mathbf{Z}_p$ is a field and accordingly the characteristic of $\mathbf{Z}_p$ is $p$. One of the consequences of the above property is that $p = 0$ in the field for any $\alpha$ in the field.



$\mathbf{Z}_p$ is the main source of prime fields. Another class of finite fields are those whose size is a power of prime, we will consider this class later.

2.3 Functions and Chinese Remainder Theorem

**Definition**: A function is defined by a triplet $< X, Y, f >$, where $X$: a set called domain; $Y$: a set called range or codomain and $f$: a rule which assigns to each element in $X$ precisely one element in $Y$.



It is denoted by $f : X \rightarrow Y$

Example: Let $X = Y = \mathbf{Z}_5$, Then $f : X \rightarrow Y$ given by $f(x) = 2 * x$ is a function.

**Image** : If $x \in X$, the image of $x$ in $Y$ is an element $y \in Y$ such that $y = f(x)$.
**Pre-image** : If $y \in Y$, then a Pre-image of $y$ in $X$ is an element $x \in X$ such that $f(x) = y$.



**Image of a function** $f$ ($Im(f)$): A set of all elements in $Y$ which have at least one Pre-image.

$$Im(f) = \bigcup_{x \in X} \{f(x)\} \tag{1}$$

# One-to-one (injective) Function

A function is one-to-one (injective) if each element in the codomain $Y$ is the image of **at most** one element in the domain $X$. In other words, each element in $x$ in $X$ is related to different $y$ in $X$, never two different elements in $X$ map to a same element in $Y$. We can say that $|X| \leq |Y|$. An alternate definition would be, a $f : X \to Y$ is one-to-one (injective), provided

$$f(x_1) = f(x_2) \text{ implies } x_1 = x_2.$$

**Examples:** Let $X = Y = \mathbf{Z}_4$. Then $f : X \to Y$ given by $f(x) = 3 * x$ is a one-to-one function. However $f(x) = x^2$ is a not a one-to-one function.

A function is Onto (surjective) if each element in the codomain $Y$ is the image of **at least** one element in the domian $X$.

A function $f : X \to Y$ is onto if $Im(f) = Y$

We can say that, if $f$ is onto then $|Y| \leq |X|$.

**Example:** Let $X = Y = \mathbf{Z}_5$, Then $f : X \to Im(f)$ given by $f(x) = x^2$ is a onto function.

**Bijection**: A function which is both one-to-one and onto.

In this case, we have $|X| \leq |Y|$ and $|Y| \leq |X|$. This implies $|X| = |Y|$.

If $f : X \to Y$ is one-to-one then $f : X \to Im(f)$ is a bijection.

If $f : X \to Y$ is onto and $X$ and $Y$ are finite sets of the same size then $f$ is a bijection.

Let $m$ and $n$ are relatively prime number, $X = \mathbf{Z}_{mn}$, $Y = \mathbf{Z}_m \times \mathbf{Z}_n$. Then the mapping



$$f : X \to Y, f(x) = ((x \bmod m), x \bmod n),$$

is a bijection.

**Example:** $X := \mathbf{Z}_6$, $Y = \mathbf{Z}_2 \times \mathbf{Z}_3$. The function $f$ given below is a bijection:



| $X = \mathbf{Z}_6$ | $\to$ | $\mathbf{Z}_2 \times \mathbf{Z}_3$ |
|---|---|---|
| 0 | $\to$ | $(0,0)$ |
| 1 | $\to$ | $(1,1)$ |
| 2 | $\to$ | $(0,2)$ |
| 3 | $\to$ | $(1,0)$ |
| 4 | $\to$ | $(0,1)$ |
| 5 | $\to$ | $(1,2)$ |





Table: $f : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$

Let $n_1, n_2$ be pair-wise relatively prime integers, the system of simultaneous congruences



$$x \equiv a_1 \ (mod \ n_1),$$

$$x \equiv a_2 \ (mod \ n_2),$$

has a unique solution modulo $n = n_1 \ n_2$.

Note that the mapping $f : \mathbf{Z}_{n_1 \; n_2} \rightarrow \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2}$ given by $f(x) \rightarrow x \; mod \; n_1, \; x \; mod \; n_2$ is a bijection.
The proof has two points. First show that the function is one-to-one. If there exists two elements $x$ and $y$ such that



$$x \; mod \; n_1 = y \; mod \; n_1,$$

and



$$x \; mod \; n_2 = y \; mod \; n_2,$$

then $x - y$ is divisible by both $n_1$ and $n_2$. Since $n_1$ and $n_2$ are relatively prime, $x - y$ is divisible by $n_1 \; n_2 = n$. Hence $x$ and $y$ are identical equal modulo $n$. This proves that the function is one-to-one. In the next slide, we give an explicit construction for the inverse function which proves that the map is onto. Hence the $f$ is bijection.

In fact, Chinese Remainder theorem gives a construction method to obtain the inverse function. Let

$$N_1 = n/n_1 = n_2, N_2 = n/n_2 = n_1.$$



Choose

$$M_1 = (N_1)^{-1} \ (mod \ n_1)$$

and



$$M_2 = (N_2)^{-1} \ (mod \ n_2)$$

.

Then the solution to the simultaneous congruences is given by



$$x = a_1 \ (N_1 \ M_1) \ + a_2 \ (N_2 \ M_2) \ \ (mod \ n).$$

You can immediately verify that $x$ determined as above satisfies the congruences (This is because $N_1 \ mod \ n_2 = 0$ and $N_2 \ mod \ n_1 = 0$)

If $n_1, n_2, \ldots, n_k$ are pair-wise relatively prime integers, k being a positive integer, the system of simultaneous congruences



$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1), \\ x &\equiv a_2 \ (mod\ n_2), \\ x &\equiv a_3 \ (mod\ n_3), \\ &\cdots \\ x &\equiv a_k \ (mod\ n_k), \end{aligned}$$



has a unique solution modulo $n = n_1\ n_2\ \ldots\ n_k$.

Let

$$N_i = n/n_i$$

for $i = 1, 2, \ldots, k$.

Choose

$$M_i = (N_i)^{-1} \ (mod \ n_i),$$

for $i = 1, 2, \ldots, k$.

Then the solution is given by

$$x = \sum_{i=1}^{k} a_i N_i M_i \ (mod \ n)$$

Lecture 1
Modern Symmetric key Ciphers



**Lecture 2**
**Properties of Numbers III**



Workshop 3: Workshops based on Lectures in Week 2

Quizz 3