Week 3

Lecture 2

Properties of Numbers III

University of Melbourne

Lecture 1
Modern Symmetric key Ciphers

Lect
Pro

Workshop 3: Workshops based on Lectures in We

Quizz 3

2.1

2.2

2.3

Recap

- Numbers, Divisibility, Mod Operation, GCD, Extended GCD
- Inverse Mod n
- Properties Euler's Phi (ϕ) Function
-
- $a \geq 1$.
-
- In fact, $\phi(mn) = \phi(m)\phi(n)$, for any t relatively prime.

let $\mathbf{Z}_n^\star$ be set of numbers from 1 to n

Theorem

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

Using Extended GCD Algorithm

Function(a, n)

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

If g eq 1 then Return(x)

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.

2.1

Euler's Theorem

Definition

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

How
the se

Defi

Reduced set of residues mod n: For n 1, the reduced set of residues, R(n) is defined as set of residues mod 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 $a\,R(n) = \{a\,r_1, a\,r_2, \ldots, a\,r_{\phi(n)}\}$. Sinc … l to $R(n)$ … s the resid … $R(n)$ and equate with the multiplication of all the elements of $a\,R(n)$. Hence we can write:

$$r_1 \times r_2 \cdots \times r_{\phi(n)} = (a r_1) \times \ldots$$

Note that r_is 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

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

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

Theorem

If a

The

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 e

Fer

Theorem

Let p be a prime number,

$$a^p = a \ (mod \ p), \ for \ an$$

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

- p
-
- Hence $\mathbf{Z}_p$ is closed under addition and p .
- In fact, $\mathbf{Z}_p$ is a finite field, a structure exte Cryptography.

Assignment Project Exam Help

2.2 https://eduassistpro.github.i

Add WeChat edu_assist_pr

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 $a, b, c \in G$
- $\in G$,

- For each $a \in G$, there exists an *inverse* element a G such that

$$a \cdot a^{-1} = a^{-1} \cdot$$

- 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, such that:

-
- $, c \in R$.
- The *distributive laws* hold; that is , for al ve $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b$

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.
- as an

-

distributive.

In $\mathbf{Z}_p$, unlike in Integers, p times any ele the field. This leads to a concept called "characteri

We also denote $\mathbf{Z}_p^\star$ as a set of non-zero elements of $\mathbf{Z}_p$.

Characteristic of F

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

integ

real and complex fields is 0.

In contrast for residue class rings $\mathbf{Z}_n$, th

When n is prime, $\mathbf{Z}_p$ is a field and according

$\mathbf{Z}_p$ is p. One of the consequences of the above pro

$p = 0$ in the field for any α 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

Definition: A function is defined by a triplet $< X, Y, f >$, where

X: a set c

f: a rule ment

in Y

It is den

Example: Let $X = Y = \mathbf{Z}_5$, Then f :

$f(x) = 2 * x$ 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- ent

$x \in$

Ima which

have a

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

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, ne Y.
We ca
$f : X$

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

Examples: Let $X = Y = \mathbf{Z}_4$. Then f
$f(x) = 3 * x$ is a one-to-one function. Howev
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 X .

Exa

$f(x)$

Bije

In this case, we have $|X| \leq |Y|$ and $|Y|$

$|X| = |Y|$.

If $f : X \to Y$ is one-to-one then $f : X \to I$

If $f : X \to Y$ is onto and X and Y are finit n f is a bijection.

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

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		$(0, 0)$
4	$\to$	
5	$\to$	

Table: $f : \mathbf{Z}_6 \to \mathbf{Z}$

Let n_1, n_2 be pair-wise relatively prime integers, the system of simu

$$x \equiv a_2 \ (mod\ n$$

has a unique solution modulo $n = n_1$

Note that the mapping $f : \mathbf{Z}_{n_1 \ n_2} \to \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2}$ given by $f(x) \to x \ mod \ n_1, \ x \ mod \ n_2$ 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

then $x - y$ is divisible by both n_1 and relatively prime, $x - y$ is divisible by n are identical equal modulo n. This proves that th one-to-one. In the next slide, we give an explicit cons 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

1

and

.

Then the solution to the simultaneous congruen

$$x = a_1 (N_1 M_1) + a_2 (N_2$$

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

$$\equiv \quad 3 \qquad 3$$

$$\dots$$

$$x \equiv a_k \ (mod\ n$$

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

Let

$$N_i = n/n_i$$

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

Choose

for i

The

$$x = \sum_{i=1}^{k} a_i N_i M_i$$

Week 3

Lecture 1
Modern Symmetric key Ciphers

Lect
Pro

Workshop 3: Workshops based on Lectures in We

Quizz 3