Week 1

Lecture 2

Introduction to Numbers

University of Melbourne

Overview Lecture

Subject Overview

Lecture 1

Lecture 2

Introduction to Numbers

Quizz 1

Workshops start from Week 2

2.1 Fu

Sets

A set is a collection of objects. The objects are referred to as elements of the set.

Example

$X = \{a, b, c\}$ is a set with three elements a, b and c.

		ol Used
Na		N
Integers	$\{\cdots, -2, -1, 0,$	
Positive Integers	$\{1, 2, 3, \ldots$	
Negative Integers	$\{\ldots, -2,$	

Table: Examples of Sets

Main Source of Finite Sets

The set of integers is a major source of finite sets.

For ex

$n -$

The properties of such finite sets play a vital role in cod

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

- X: a set called domain;
- Y: a set called range or codomain and
- ne

Exa

$$[0,1]^K \to [0,$$

Where the message domain is all binary vectors of le d the codomain is a space of N bit numbers.

Example from Cryptographic Functions

- Alphabet, $\mathcal{A}$: A finite set. For example, $\mathcal{A} = \{0, 1\}$, the binary alphabet.
- Message Space, $\mathcal{M}$: Consists of strings of symbols from an
- Key space $\mathcal{K}$: A set of key space and an eleme .
- Encryption function, E_e:
$$C = E_e(M$$
- Decryption function, D_d:
$$M = D_d(C)$$

2.2 Di

- Division Theorem

Divisibility

An integer "a" is said to be **divisible** by a positive integer "b", and this is written as $b|a$, if $a = bc$ for a third integer "c" and $c \neq 0$.
(The above statement is also same as "b" divides "a".)
In the f

1.
2.
3. $a|b$ and $b|a$ implies $a = \pm b$,
4. $a|b$ and $a|c$ implies $a|(bx + cy)$ for any x and y,
5. $a|b$ implies $ca\ |cb$, for any c.

Proof of (4).

Sinc $a|c$,
we ca
$b\ x$
$a|b\ x + c\ y$. □

Division with Remainder

Let a, b be two integers, $a > b$

b does not divide a ;

The l le of
b;

where $c = q\ b < a$;
then

$$a = c + r = q\ b$$

q is the quotient and r is called as **remainder modulo** b.

Finding Remainder and Modulo Operation

Let a be any integer b a positive integer which is not zero, then are unique integers q (quotient) and r (remainder) such that

$$a = qb + r, 0 \quad r < b.$$

The q
repre
than or equal to x. The remainder r is written as

$$r = a \mod$$

Example: $12 \bmod 5 = 2$.
$-12 \bmod 5 = 3$.

Division Theorem

Theorem

Let a and b are integers and assume that b is positive. Then there exist integers q and r such that

Proo

For fixed a and b, let X be the collection of integers of the form $a - xb$. Let r be the least non-negative integ be the corresponding integer, so that $a -$

Claim: $0 \leq r < b$.

Note that this follows from the well-ordering principle.

Now we need to examine the uniqueness of q and r:

□

Proof Cont.

Suppose they are not unique, then we have $q\ b + r\ =\ q'\ b + r'$.
WLG (Without loss of generality) : $r \leq r'$.
Then, $(q - q')\ b = (r' - r)$ and $r' - r \geq 0$.
If $(r' - r) \neq 0$, then necessarily $(q - q') > 0$.
If so then

.

But
So we have

$$b \leq r' - r$$

This is a contradiction to $r \neq r'$.
Therefore $r = r'$ and
subsequently, $q = q'$.

2.3 Pr

Prime Numbers

Definition

A number is said to be **a prime number** *if $p > 1$ and p has no positive divisors except 1 and p.*

Defi

The n
com

Fact

There are infinitely many prime numbers.

Can you prove this? There is a simple proof originally attributed to Euclid.

Prime Numbers

Fact

There are infinitely many prime numbers.

We kn n prim prim gest prime in the set and none of them divides Q. If Q is a prime number, we are done with the proof. If not, there exist prime q which divides Q. q cannot be on and has to be a new prime greater than the proof.

Greatest Common Divisor (GCD)

Definition

If d divides two integers m and n, then d is called a common divisor. The greatest of common divisors of the integers is the GCD

Defi

Numbers m and n are said to be relatively pri *m and n is 1.*

Example: $gcd(3, 5) = 1$
$gcd(2, 14) = 2$;

A useful theorem

Theorem

Let a, b, q, r be integers with such that $a = qb + r$. Then $gcd(a, b) = gcd(b, r)$.

Proo

If a e
true.
$d|a - qb$ (the divisibility property (4)). So,
divisor of both b and r. Now let c be a d $|b$
and $c|r$. Then again from the divisibility propert , so
$c|a$. This means that c is a common diviso d.
This implies that $d = gcd(b, r)$.
Thus, we have proved $gcd(a, b) = gcd(b, r)$. □

2.4 GCD Computation

-
-
-
-
- Modular Multiplicative Inverse
- Fundamental Theorem of Arithmeti

Key Fact for GCD computation

There is an algorithm to compute gcd which is considered as one of the earliest known algorithms, familiar in many cultures. It is known as Euclidean algorithm in modern textbooks.

Fact

Let

$$gcd(a, b) = gcd(b, ($$

From the basic fact remainder ng, we have $r = a \ mod \ b$ is the remainder. It is clear that a co a and b is divisor of r too and the result is obvious.

Euclid's algorithm


```
Euclid(a,b);
X:=a
whil
r = x mod y;
x:=y
y:=r; }
return(x);
```

$gcd(33, 21)$

Table: Determination of

GCD Illustration through Manual Computations

Consider $gcd(33, 21)$:

$$\begin{array}{rcll} 33 & = & 1 \times 21 + 12 & gcd(21, 12) \quad (A) \\ 21 & = & 1 \times 12 + 9 & gcd(12, 9) \quad (B) \\ 12 & = & 1 \times 9 + 3 & gcd(9, 3) \quad (C) \\ 9 & = & 3 \quad 3 + 0 & gcd(3, 0) \end{array}$$

$$3 = 12 - 1 \times (21 - 1 \times 12$$

$$3 = 2 \times 12 - 1 \times 21$$

$$3 = 2 \times (33 - 1 \times 21) - 1 \times$$

$$3 = 2 \times 33 + (-3) \times 21 \qquad \textit{Simplification}$$

Note that the gcd (in this case 3) can be written as a function of its inputs (33 and 21). This is an extended Euclidean algorithm helps in computing inverses! We will study this fact next week.

Modular Arithmetic

Let a and b be integers and let n be a positive integer.
We say "a" is congruent to "b", modulo n and write

$$a \equiv b \pmod{n}$$

if a and b differ by a multiple of n; i.e ; if n is a factor of $|b - a|$.
Ever
the se

We can define the following operations:

$$x \oplus_n y = (x + y) \bmod n$$

$$x \otimes_n y = (xy) \bmod n$$

When the context is clear we use the above special addition and multiplication symbols interchangeably with their counterpart regular symbols.

Modular Multiplicative Inverse

Definition

Let $x \quad Z_n$, *if there is an integer* y *such that*

then

$y = x^{-1}$ *usually.*

Example: let $n = 5$, 2 is inverse of 3 in Z_5 because 2 is inverse of 3 modulo 5.

Determining multiplicative inverse

Fact

For any integers a and b, there exist integers x and y such that

You c

gcd(a,b). Thus we can say that we can find inverse of o *n* provided $gcd(a, n) = 1$. gcd can also determine result. Can you think how?

Fundamental Theorem of Arithmetic

Fact

Every natural number $n > 1$ has a unique prime factorization or prime power factorization.

wher

Example:

$15 = ?$

$32 = ?$

$2^{607} - 1 = ?$

$3937 = ?$

Fundamental Theorem of Arithmetic

Fact

Every natural number $n > 1$ has a unique prime factorization or prime power factorization.

wher

Example:

$15 = 5 * 3$

$32 = 2^5$

$2^{607} - 1 = 1\ (2^{607} - 1)$

$3937 = 127 * 31$

Overview Lecture

- Subject Overview

Lecture 1

Introduction to cryptography.

Lect

Intr

2.1

2.2 **Division and Remainders**

2.3 **Prime Numbers**

2.4 **GCD computation**

Quizz 1

Workshops start from Week 2