Cryptography:Mathematical Foundation
Properties of Numbers

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne

January, 2016

THE UNIVERSITY OF MELBOURNE

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.

Name	Set	Symbol Used
Natural Numbers	$\{0, 1, 2, 3, \cdots\}$	N
Integers	$\{\cdots, -2, -1, 0, +1, +2, \cdots\}$	Z
Positive Integers	$\{1, 2, 3, \cdots\}$	$Z+$
Negative Integers	$\{\cdots, -2, -1\}$	$Z-$

Table: Examples of Sets

Main Source of Finite Sets

The set of integers is a major source of finite sets.
For example, for a positive integer n, the set of numbers from 0 to $n-1$ form a finite set of n entities denoted by Z_n.

$$Z_n := \{0, 1, 2, \cdots n-1\}$$

The properties of such finite sets play a vital role in cryptography.

Functions

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 $f : X \to Y$

Example: Hash Function: h.

$$[0, 1]^N \to [0, 1]^{128},$$

Where message domain is all binary vectors of length N and codomain is a space of 128 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 alphabet.
- Cipher Text Space, $\mathcal{C}$: Consists of strings of symbols from an alphabet which may differ form the alphabet of $\mathcal{M}$.
- Key space $\mathcal{K}$: A set of key space and an element of $\mathcal{K}$ is key.
- Encryption function, E_e: A mapping from $\mathcal{M}$ to $\mathcal{C}$ determined by the key e.
- Decryption function, D_d: An inverse mapping from $\mathcal{C}$ to $\mathcal{M}$ determined by the key d.

Divisibility

An integer "a" is said to be divisible by a positive integer "b". not "0" if there exists ($\exists$) a third integer "c" such that ($\ni$)

$$a = b\ c$$

We simply write sometimes $b|a$.
Let a, b be two integers, $a > b$

$$b \text{ does not divide } a\ ;$$

Then let c be the largest integer smaller than a and is multiple of b;

$$b|c,$$

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

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

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

Some properties of divisibility

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

Some properties of divisibility, cont

Proof of (4).

Since $a|b$, we have $b = ma$ for some integer m. Similarly since $a|c$, we can write $c = na$ for some integer n. Now consider $b\ x + c\ y = m\ a\ x + n\ a\ y = a(m\ x + n\ y)$. Therefore $a|b\ x + c\ y$. $\square$

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

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

The quotient q can be obtained by $q = \lfloor a/b \rfloor$, where $\lfloor x \rfloor$, represents the floor function which returns the largest integer less than or equal to x. The remainder r is written as

$$r = a \mod b.$$

Example: 12 mod 5 $= 2$.
-12 mod 5 $= 3$.

Division Theorem

Theorem

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

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

Proof.

For fixed a and b, let X be the collection of integers of the form $a - xb$. Let r be the least non-negative integer in X, and let q be the corresponding integer, so that $a - q\ b\ =\ r$.
Claim: $0 \leq r < b$.
Note that this follows from the well-ordering principle.
Now we need to examine 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

$$r' - r = (q - q')\ b \geq 1\ b$$

.
But $r' - r \leq r' < b$
So we have

$$b\ \leq\ r' - r\ < b$$

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

$\square$

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.*

Composite Numbers::

Definition

The numbers which are not prime numbers are referred as **composite numbers**.

Fact

Every positive integer exceeding 1 is a product of prime numbers.

Fact

There are infinitely many prime numbers.

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

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 of m and n.

Definition

Numbers m and n are said to be relatively prime if the GCD of m and n is 1.

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

A useful theorem

Theorem

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

Proof.

If a and b are identically zero, then $r = 0$ and the result is trivially true. Otherwise let $d = gcd(a, b)$. Since $d|a$ and $d|b$, we have $d|a - qb$ (the divisibility property (4)). So, $d|r$ and d is a common divisor of both b and r. Now let c be a divisor of b and r. i.e $c|b$ and $c|r$. Then again from the divisibility property (4), $c|qb + r$, so $c|a$. This means that c is a common divisor of a and b. So, $c \leq d$. This implies that $d = gcd(b, r)$.
Thus, we have proved $gcd(a, b) = gcd(b, r)$. $\square$

gcd computation

There is an algorithm to compute gcd which is considered as one of the earliest known algorithms. This has been attributed to Euclid of ancient Greece.

Fact

Let $a > b > 0$. Then

$$gcd(a, b) = gcd(b, (a \ mod \ b)).$$

From the basic fact remaindering, we have $a = qb + r$, where $r = a \ mod \ b$ is the remainder. It is clear that a common divisor of a and b is divisor of r too and the result is obvious.

Euclid's algorithm

```
Euclid(a,b);
X:=a; y:=b;
while y > 0 do {
r = x mod y;
x:=y;
y:=r; }
return(x);
```

Euclid's algorithm

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

Table: Determination of $gcd(33,21)$

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

同余

$$a \equiv b \ (mod \quad n),$$ (a-b)能够被n整除

if a and b differ by a multiple of n; i.e ; if n is a factor of $|b - a|$.
Every integer is congruent mod n to exactly one of the integers in the set

$$Z_n = \{0, 1, 2, \cdots, n - 1\}.$$

We can define the following operations:

$$X \oplus_n y = (x + y) \ mod \ \ n.$$

$$X \otimes_n y = (xy) \ mod \ \ n$$

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 $x \in Z_n$, if there is an integer y such that

$$X \otimes_n y = 1,$$

then we say y is the multiplicative inverse of x. It is denoted by $y = x^{-1}$ usually.

Example: let $n = 5$, 2 is inverse of 3 in Z_5. Or in other words 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

$$gcd[a, b] := ax + by.$$

You can determine x and y by modifying Euclid's algorithm for gcd(a,b). Thus we can say that we can find inverse of a modulo n provided $gcd(a, n) = 1$. gcd can also determined from next result. Can you think how?

Fundamental Theorem of arithmetic

Fact

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

$$n = \Pi_{i=1}^{\tau} p_i^{a_i},$$

where τ is a positive number.

Example:
$15 = 5\ 3$
$32 = 2^5$
$2^{607-1} = 1\ (2^{607} - 1)$
$3937 = 127 * 31$