Cryptography
And
Cryptanalysis

Ph. D. Course/ 2019-2020

Introduced By

Dr. Faez Hassan Ali

Lecture One

Mathematical Basic Concepts

The following notation will be used throughout:

- Z denotes the set of integers; that is, the set $\{\ldots,-2,-1,0,1,2,\ldots\}$.
- Q denotes the set of rational numbers; that is, the set $\{\ |a,b\in Z,b\neq 0\}$.
- R denotes the set of real numbers.
- $[a, b]$ denotes the integers x satisfying $a \le x \le b$.
- $a\in A$ means that element a is a member of the set A.
- $A\subseteq B$ means that A is a subset of B.
- $A\subset B$ means that A is a proper subset of B; that is $A\subseteq B$ and $A\neq B$.
- The intersection of sets A and B is the set $A\cap B=\{x|x\in A \text{ and } x\in B\}$.
- The union of sets A and B is the set $A\cup B = \{x|x\in A \text{ or } x\in B\}$.
- The difference of sets A and B is the set $A-B = \{x|x\in A \text{ and } x\notin B\}$.
- The Cartesian product of sets A and B is the set $A\times B=\{(a,b)|a\in A \text{ and } b\in B\}$.
- $\sum_{i=1}^{n} a_i$ denotes the sum $a_1+a_2+\ldots+a_n$.
- $\prod_{i=1}^{n} a_i$ denotes the product $a_1.a_2.\ldots.a_n$.
- For a positive integer n, the factorial function is $n!=n(n-1)(n-2)\ldots1$. By convention, $0! = 1$.

Number Theory - Primality

<u>Definition (2.1)</u>: A positive integer n>1 that has only two distinct factors, 1 and n itself (when these are different), is called ***prime***; otherwise, it is called **composite**.

<u>Remark (2.2)</u>:

- It is interesting to note that primes thin out: there are eight up through 20, but only three between 80 and 100.
- Note that 2 is the only even prime, all the rest are odd.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Number Theory - Multiplicativity

<u>Theorem</u>: the fundamental theorem of arithmetic

Any positive integer n>1 can be written uniquely in the following prime factorization form:

n=$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$

where $p_1<p_2<\ldots<p_k$ are primes, and $\alpha_1,\alpha_2,\ldots,\alpha_k$ are non negative integers. Example:

$$\begin{array}{lll} 1999 = 1999, & 2000 = 2^4.5^3, & 2001 = 3.23.29 \\ 2002 = 2.7.11.13, & 2003 = 2003, & 2004 = 2^3.3.167 \\ 2005 = 5.401, & 2006 = 2.17.59, & 2007 = 3^2.223 \\ 2008 = 2^3.251, & 2009 = 7^2.41, & 2010 = 2.3.5.67 \end{array}$$

Number Theory - Divisibility

Definition (2.2): Let a and b be two integers, not both zero. The largest divisor d s.t. d|a and d|b is called the **greatest common divisor** (gcd) of a and b, which is denoted by gcd(a,b).

Definition (2.3): Let a and b be two integers, not both zero. d is a common multiple of a and b, the least common multiple (lcm) of a and b, is the **smallest common multiple**, which is denoted by lcm(a,b).

Definition (2.4): Integers a and b are called **relatively prime** if gcd(a,b)=1. we say that integers $n_1,n_2,\ldots n_k$ are relatively prime if, whenever $i\neq j$, we have $\gcd(n_i,n_j)=1$, $\forall i,j$, $1\leq i,j\leq k$.

Theorem (2.2): Suppose a and b are two positive integers.

If $a=\prod_{i=1}^{k} p_i^{\alpha_i}$ and $b=\prod_{i=1}^{k} p_i^{\beta_i}$, then

$\gcd(a,b)=\prod_{i=1}^{k} p_i^{\varepsilon_i}$, where $\varepsilon_i=\min(\alpha_i,\beta_i)$, $\forall i$, $1\leq i\leq k$.

$\mathrm{lcm}(a,b)=\prod_{i=1}^{k} p_i^{\delta_i}$, where $\delta_i=\max(\alpha_i,\beta_i)$, $\forall i$, $1\leq i\leq k$.

Example (2.2): Since the prime factorization of 240 and 560 are:

$240=2^4.3.5$ and $560=2^4.5.7$, then the:

$\gcd(240,560)=2^{\min(4,4)}.3^{\min(1,0)}.5^{\min(1,1)}.7^{\min(0,1)}=2^4.3^0.5^1.7^0=80.$

$\mathrm{lcm}(240,560)= 2^{\max(4,4)}.3^{\max(1,0)}.5^{\max(1,1)}.7^{\max(0,1)}=2^4.3^1.5^1.7^1=1680.$

Theorem (2.3): Suppose a and b are two positive integers, then

$\mathrm{lcm}(a,b)=\dfrac{a.b}{\gcd(a,b)}$.

Euclidean Algorithm

Fact (2.1) If a and b are positive integers with a>b, then:

gcd(a,b)=gcd(b, a mod b). The Euclidean algorithm:

- **INPUT**: two non-negative integers a and b with a ≥ b.
- **OUTPUT**: the gcd of a and b.
- 1. **WHILE** $b \neq 0$ **DO** the following:
- 1.1 Set $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
- 2. **RETURN**(a).
- **Example(2.3)**:for computing gcd(4864,3458)
- $4864 = 1 \cdot 3458 + 1406$
- $3458 = 2 \cdot 1406 + 646$
- $1406 = 2 \cdot 646 + 114$
- $646 = 5 \cdot 114 + 76$
- $114 = 1 \cdot 76 + 38$
- $76 = 2 \cdot \mathbf{38} + 0$.
- Then gcd = 38.

The integers modulo n

Let n be a positive integer.

<u>Definition</u>: If a and b are integers, then a is said to be congruent to b modulo n, written: $a \equiv b \pmod{n}$, if n divides $(a-b)$. The integer n is called the modulus of the congruence.

<u>Example</u>

- $24 \equiv 9 \pmod{5}$ since $24 - 9 = 3 \cdot 5$.
- $-11 \equiv 17 \pmod{7}$ since $-11 - 17 = -4 \cdot 7$.
- if $a = qn + r$, where $0 \le r < n$, then $a \equiv r \pmod{n}$.

<u>Definition:</u> The integers modulo n, denoted Z_n, is the set of (equivalence classes of) integers$\{0,1,2,...,n-1\}$. Addition, subtraction, and multiplication in Zn are performed modulo n.

<u>Example:</u> $Z_{25} = \{0,1,2,...,24\}$.In Z_{25},

$13+16=4$, since $13+16=29 \equiv 4 \pmod{25}$. Similarly, $13 \cdot 16 = 8$ in Z_{25}.

Arithmetic Functions

Definition: A **function** f is a rule that assigns to each element in a set D (called **Domain** of f) one and only one element in a set B. the set of images called the **range** (R) of f.

Definition: The function f has the property of being "**one-to-one**" (or "**injective**") if no two elements in D are mapped into the same element in R.

The function f has the property of being "**onto**" (or "**surjective**") if the range R of f is all of B (R=B).

Definition : Given functions f and g, the **composition** of f with g, denoted by $f \circ g$ is the function by: $(f \circ g)(x)=f(g(x))$, The domain of $f \circ g$ is defined to consists of all x in the domain of g for which $g(x)$ is in the domain of f.

Definition : A function f is called an **arithmetic function** or a **number theoretic** function if it assigns to each positive integer n a unique real or complex number $f(n)$. Typically, an arithmetic function is a real-valued function whose domain is the set of positive integer.

Example: the equation $\sqrt{n}$, $n \in N$, defines an arithmetic function f which assigns the real number $\sqrt{n}$ to each positive integer.

Definition : A real function defined on the positive integers is said to be **multiplicative** if: $f(m)f(n)=f(mn)$, $\forall m,n \in N$ with $\gcd(m,n)=1$.

Arithmetic Functions

Definition: Let n be a positive integer. **Euler's** Φ-function, $\Phi(n)$ defined to be the number of positive integer k less than n which are relatively prime to n:

$$\Phi(n)= \sum_{\substack{1\le k<n \\ \gcd(k,n)=1}} 1$$

Example: By definition:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	40	100	32	102

Theorem : Let $n\in Z^+$, then $\Phi(n)$ is multiplicative i.e. $\Phi(mn)= \Phi(m)\,\Phi(n)$.

if n is prime, say p, then $\Phi(p)=p-1$, and if n is prime power p^α, then

- $\Phi(p^\alpha)= p^\alpha- p^{\alpha-1}= p^{\alpha-1}(p-1)$.
- if n is composite and has the standard prime factorization form, then
- $\Phi(n)= \prod_{i=1}^{k} p_i^{\alpha_i-1}(p_i-1)$
- $\Phi(n)=(p-1)(q-1)$ if n=pq, where p and q are prime numbers.

Definition: Let $x \in R^+ \ge 1$, then $\pi(x)$ is defined as follows: $\pi(x)= \sum_{\substack{p\le x \\ p \text{ prime}}} 1$

$\pi(x)$ is called the **prime counting** function (or the **prime distribution function**).

Example: $\pi(1)=0$, $\pi(2)=2$, $\pi(10)=4$, $\pi(20)=8$, $\pi(50)=15$, $\pi(75)=21$, $\pi(100)=25$.