Lecture One

Mathematical Basic Concepts

2. Number Theory

Number theory, in mathematics, is primarily the theory of the properties of integers (whole numbers) such as parity, **divisibility**, **primality**, **additivity**, and **multiplicativity**, etc. In the next subsections we will investigate more detailed discussions about numbers.

2.1 Primality

Definition (2.1): 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**. The first few prime numbers are: 2,3,5,7,11,13,17,….

Remark (2.2):

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

Remark (2.3):

Sieve of Eratosthenes is a method is found to specify the prime numbers. This method depends on cancelling all multiples of 2,3,5,7,…within the specified range, for example if we want to know all primes between 0 and 99:

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

The primes are (not shaded): 2,3,5,7,11,13,…,83,89,97.

2.2 Multiplicativity

Theorem (2.1): (**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 (2.1): The following are prime factorization of n for n=1999, 2000, …, 2010.

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

2.3 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 $n_1,n_2,\dots n_k$ are relatively prime if, whenever $i\neq j$, we have $\gcd(n_i,n_j)=1$, $\forall i,j,\ 1\le i,j\le k$.

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 $\varepsilon_i=\min(\alpha_i,\beta_i)$, $\forall i,\ 1\le i\le k$.

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

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:

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

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

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

$$\operatorname{lcm}(a,b)=\frac{a.b}{\gcd(a,b)}.$$

2.4 Euclidean Algorithm

The Euclidean algorithm is an efficient algorithm for computing the greatest common divisor of two integers that does not require the factorization of the integers. It is based on the following simple fact.

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 steps are: computing the gcd of two integers:

INPUT: two non-negative integers a and b with a ≥ b.

OUTPUT: the gcd of a and b.

1. **WHILE** b≠0 **DO** the following:

    1.1 Set r←a mod b, a←b, b←r.

2. **RETURN**(a).

Example(2.3) (Euclidean algorithm):for computing gcd(4864,3458)=38

4864 = 1·3458 + 1406
3458 = 2·1406 + 646
1406 = 2·646 + 114
646 = 5·114 + 76
114 = 1·76 + 38
76 = 2·38 + 0.

2.5 The integers modulo n

Let n be a positive integer.

Definition (2.5): 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.

Example (2.4):

i. $24 \equiv 9 \pmod{5}$ since $24 - 9 = 3 \cdot 5$.

ii. $-11 \equiv 17 \pmod{7}$ since $-11 - 17 = -4 \cdot 7$.

Fact (2.2) (***properties of congruence's***) $\forall\ a, a_1, b, b_1, c \in Z$, the following are true.

i. $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.
ii. (***reflexivity***) $a \equiv a \pmod{n}$.
iii. (***symmetry***) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
iv. (***transitivity***) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
v. If $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$, then $a+b \equiv a_1+b_1 \pmod{n}$ and $ab \equiv a_1 b_1 \pmod{n}$.

The equivalence class of an integer a is the set of all integers congruent to a modulo n. From properties (ii), (iii), and (iv) above, it can be seen that for a fixed n the relation of congruence modulo n partitions Z into equivalence classes. Now, if a = qn + r, where $0 \le r < n$, then $a \equiv r \pmod{n}$. Hence each integer a is congruent modulo n to a unique integer between 0 and n−1, called the least residue of a modulo n. Thus a and r are in the same equivalence class, and so r may simply be used to represent this equivalence class.

Definition (2.6): The integers modulo n, denoted Z_n, is the set of (equivalence classes of) integers $\{0,1,2,\ldots,n-1\}$. Addition, subtraction, and multiplication in Zn are performed modulo n.

Example(2.5): Z_{25} ={0,1,2,...,24}.

In Z_{25}, 13+16=4, since 13+16=29≡4 (mod 25). Similarly, 13·16 = 8 in Z_{25}.