# Chapter 8 Number Theory

**8-1 Prime Numbers and Composite Numbers**

***d* divides *n*, *d*|*n*:** $n=dq$, $d$ ($\neq 0$) is a divisor (factor) of $n$, and $q$ is the quotient.

**Eg. 2|6, 3|108, etc.**

**Theorem Let *m*, *n*, and *d* be integers. (a) If *d*|*m* and *d*|*n*, then *d*|(*m*±*n*). (b) If *d*|*m*, then *d*|*mn*.**

(Proof) (a) $\because m=dq_1$ and $n=dq_2$, $\therefore m\pm n=d(q_1\pm q_2)$.

(b) $m=dq$, and then $mn= dnq$

**Prime number:** An integer greater than 1 whose only positive divisors are itself and 1.

**Eg. 2=1×2, 3=1×3, 5=1×5, 7=1×7, 11=1×11, … are all prime numbers.**

**Composite number:** An integer greater than 1 that is not prime.

**Eg. 4=1×4=2×2, it is a composite number.**

**Theorem A positive integer *n* greater than 1 is composite if and only if *n* has a divisor *d* satisfying $2\leq d\leq \sqrt{n}$ .**

(Proof) ($\Rightarrow$): Suppose that $n$ is composite, $n$ has a divisor $d'$ satisfying $2 \leq d' \leq n$.

If $d' \leq \sqrt{n}$, then $n$ has a divisor $d=d'$ satisfying $2 \leq d \leq \sqrt{n}$.

If $d'>\sqrt{n}$, then $n=d'q$, Thus $q$ is also a divisor of $n$. Suppose that $q>\sqrt{n}$, then $n=d'q>\sqrt{n}\cdot\sqrt{n}=n$, which is a contradiction. Thus $q<\sqrt{n}$. Therefore, $n$ has a divisor $d= q$ satisfying $2 \leq d \leq \sqrt{n}$.

($\Leftarrow$): If $n$ has a divisor $d$ which satisfies $2 \leq d \leq \sqrt{n}$, according to the definition of composite number, $n$ is composite.

**Algorithm Testing whether an integer is prime**

```
  Input: n
 Output: d
is_prime(n) {
  for d = 2 to ⌊√n⌋
    if (n mod d == 0)
      return d
  return 0
}
```

**Theorem There are infinite prime numbers.**

(Sol.) Assume there are only finite prime numbers: $p_1, p_2, p_3, \ldots, p_n$.

Let $m = p_1 p_2 p_3 \ldots p_n + 1$, so $m$ should be a composite number.

But $m$ can not be factorized into the product of $p_1, p_2, p_3, \ldots$, and $p_n$. It should be a prime number. They are contradictory to each other.

Hence, there are infinite prime numbers.

## 8-2 GCD and LCM

**The greatest common divisor (*gcd*):** Let $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $n = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$,

then $gcd(m,n) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$.

**Eg.** $12=2^2\times 3$, $18=2\times 3^2$, $gcd(12,18)=2^{min(2,1)}\times 3^{min(1,2)}= 2\times 3=6$.

**The least common multiple (*lcm*):** Let $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $n = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$,

then $lcm(m,n) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$.

**Eg.** $12=2^2\times 3$, $18=2\times 3^2$, $lcm(12,18)=2^{max(2,1)}\times 3^{max(1,2)}= 2^2\times 3^2=36$.

**Theorem For any integers $m$ and $n$, $gcd(m,n) \cdot lcm(m,n)=mn$.**

(Proof)

$$gcd(m,n) \cdot lcm(m,n) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)} \cdot p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

$$= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} = mn.$$

**Eg.** $gcd(12,18)\times lcm(12,18)= 6\times 36=216=12\times 18$.

**Remainder $r$ of $b$ dividing $a$:** $r=a$ mod $b$.

**Eg. 12 mod 5=2.**

**Theorem If $a$ and $b$ are nonnegative integers, not both zero, then there exist integers $s$ and $t$ such that $gcd(a,b)=sa+tb$.**

**Eg.** $gcd(105,30)=15$, and we have $1\times 105+(-3)\times 30=15$.

**Euclidean Theorem If *a* is a nonnegative integer, *b* is a positive integer, and *r*=*a* mod *b*, then *gcd*(*a*,*b*)=*gcd*(*b*,*r*).**

(Proof) $a=bq+r$, $0 \le r < b$.

Let $c \mid a$ and $c \mid b$. And we have $c \mid bq$. Moreover, $c \mid (a-bq=r)$.

Let $c \mid b$ and $c \mid r$. And we have $c \mid bq$. Moreover, $c \mid (bq+r=a)$.

Thus the set of common divisors of *a* and *b* is equal to the set of common divisors of *b* and *r*. Therefore, *gcd*(*a*,*b*)= *gcd*(*b*,*r*).

**Eg. *gcd*(105,30)= *gcd*(30,15) = *gcd*(15,0)=15**

## Euclidean Algorithm

Input: *a* and *b* (nonnegative integers, not both zero)
Output: Greatest common divisor of *a* and *b*

```
gcd(a, b) {
   // make a largest
   if (a < b)
      swap(a, b)
   while (b ¬= 0) {
      r = a mod b
      a = b
      b = r
   }
   return a
}
```

**8-3 The Pigeonhole Principle (鴿籠原理)**

**The pigeonhole principle: If $m$ pigeons occupy $n$ pigeonholes and $m>n$, then at least one pigeonhole has two or more pigeons roosting in it.**

**Eg. Let $S\subset Z$, and $S$ has 37 elements. Then $S$ contains two elements that have the same remainder upon division by 36.**

(Proof) $n=36q+r$, $0\leqq r<36$. There are 36 possible values of $r$.

According to the pigeonhole principle, the result is established.

**Eg. Any subset of size six from $S=\{1,2,3,4,5,6,7,8,9\}$ must contain two elements whose sum is 10.**

(Sol.) The numbers: 1,2,3,4,5,6,7,8,9 are pigeons.

{1,9}, {2,8}, {3,7}, {4,6}, {5} are pigeonholes. When 6 pigeons go to their respective pigeons, they must fill at least one of the two-element subsets whose members sum to 10.

**Eg. Let $m$ be positive and odd. Show that there exists a positive integer $n$ such that $m$ divides $2^n$-1.**

(Proof) Consider $m+1$ integers: $2^1-1, 2^2-1, 2^3-1, \ldots, 2^m-1, 2^{m+1}-1$.

According to the pigeonhole principle, $\exists\, 1\leqq s<t\leqq m+1$ such that $2^s-1=q_1m+r$ and $2^t-1=q_2m+r$, where $1\leqq r<m$.

$(2^t-1)-(2^s-1)=2^t-2^s=2^s(2^{t-s}-1)=(q_2-q_1)m$. $\because$ $m$ is odd, $\therefore$ $gcd(2^s,m)=1$.

Hence $m\mid 2^{t-s}-1$, and the result follows with $n=t-s$.

**Eg. An inventory consists of a list of 80 items, each marked "available" or 'unavailable". There are 45 available items. Show that there are at least 2 available items in the list exactly 9 items apart.**

(Proof) Let $a_i$ denote the position of the $i^{th}$ available item.

Consider $a_1, a_2, a_3, \ldots, a_{45}$

(P1)

and $a_1+9, a_2+9, a_3+9, \ldots, a_{45}+9$.

(P2)

There are 90 numbers those have possible values only from 1 to 89. According to the pigeonhole principle, two of the numbers must coincide. Some number in (P1) is equal to some number in (P2). Therefore, $a_i-a_j=9$.