Greatest Common Divisors (GCD):

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b.
The greatest common divisor of a and b is denoted by gcd (a, b).

- One way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor.
  e.g. the positive common divisor of 24 and 36 are 1, 2, 4, 6, 12. Hence gcd (24, 36) = 12.
- The integers a and b are ***relatively prime*** if their gcd is 1.
  e.g. 12 and 25 are relative primes, since gcd(12. 25) = 1
- Another way to find the gcd is to use the prime factorization. Suppose the prime factorization of two integers a and b are
  $a = P_1^{a1}\ P_2^{a2}\ \ldots\ldots P_n^{an}$
  $b = P_1^{b1}\ P_2^{b2}\ \ldots\ldots P_n^{bn}$
  then, $\gcd(a,b) = P_1^{\min(a1,b1)} . P2^{\min(a2,b2)} \ldots\ldots\ Pn^{\min(an,bn)}$

  where $\min(x, y)$ represents the minimum of two numbers x and y.
  e.g. The prime factorizations of 120 and 500 are $120 = 2^3 . 3 . 5$ and $500 = 2^2 . 5^3$, the greatest common divisor is $\gcd(120, 500) = 2^2 . 3^0 . 5^1 = 20$

Least Common Multiple (LCM):

The LCM of the positive integers a and b is the smallest positive integer that is divisible by both a and b. the least common multiple of a and b is denoted by lcm (a, b).

- Prime factorization can also be used to find the least common multiple of two integers. The least common multiple of a and b is given by
  $\text{lcm}(a.b) = P_1^{\max(a1,b1)} . P2^{\max(a2,b2)} \ldots\ldots\ Pn^{\max(an,bn)}$

  where $\max(x, y)$ denotes the maximum of the two numbers x and y.
  e.g. the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$ is
  $\text{lcm}(2^3 3^5 7^2 , 2^4 3^3) = 2^4 3^5 7^2$
- Let a and b be two positive integers. Then,
  $ab = \gcd(a, b) . \text{lcm}(a, b)$

Modular Arithmetic:

Let a be an integer and m be a positive integer. We denote ***a* mod *m*** the remainder when a is divided by m.
Form the definition of remainder ***a* mod *m*** is the integer r such that $a = qm + r$ where $0 \leq r < m$.
e.g. 17 mod 5 = 2, -133 mod 9 = 2.

Congruence Relation: Karl Friedrich Gauss

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides a-b. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m.

- If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.
- $a \equiv b \pmod{m}$ if and only if a **mod** $m = b$ **mod** m.
- *e.g.* $17 \equiv 5 \pmod{6}$, since 6 divides 17-5 =12.
  But, 24 – 14 = 10 is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$.

Theorem:
Let m be a positive integer. The integers a and b are congruence modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b$ *(mod* m*), then* $m \mid (a-b)$.

This means there is an integer k such that $a - b = km$, $\therefore a = b + km$.
Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$.
Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$.

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Theorem let m be a positive integer. Then,

i) for any integer a, we have $a \equiv a \pmod{m}$

ii) if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

iii) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Applications of Congruence:

Pseudorandom Number: Numbers generated by systematic methods are not truly random. They are called *pseudorandom numbers*.

The most commonly used procedure for generating pseudorandom numbers is the linear congruential method. We choose four integers: the modulus m, multiplier a, increment c and seed x_0, with $2 \leq a < m$, $0 \leq c < m$, and $0 \leq x_0 < m$. We generate a sequence of pseudorandom numbers $\{x_n\}$ with $0 \leq x_n < m$ for all n, by successively using the congruence

$$x_{n+1} = (ax_n + c) \; mod \; m$$

- e.g. The sequence of pseudorandom numbers generated by choosing $m = 9$, $a = 7$, $c = 4$, and $x_0 = 3$, can be fund as follows: 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, ……

Cryptology: One of the most important applications of congruences involves cryptology, which is the study of secret messages. One of the earliest known uses of cryptology was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three). For instance, using this scheme the letter B is sent to E and the letter X is sent to A.

- To express Caesar's encryption process mathematically, first replace each letter by an integer from 0 to 25, based on its position in the alphabet. Then this encryption method can be represented by the function $f(p) = (p + 3) \; mod \; 26$ where $0 \leq p \leq 25$.
- The secret message produced from the message "*MEET YOU IN THE PARK*" using the Caesar cipher is "*PHHW BRX LQ WKH SDUN*".
- The process of determining the original from the encrypted message is called ***decryption***. The decryption function for the Caesar's cipher is $f^{-1}(p) = (p - 3) \; mod \; 26$.

Hashing Functions: A hashing function h assigns memory location h(k) to the record that has k as its key. In practice many different hashing functions are used. One of the most common is the function $h(k) = k \bmod m$ where m is the number of available memory locations.

- e.g. When $m = 111$, $h(064212848) = 064212848 \bmod 111 = 14$.
- Since a hashing function is not one-to-one, more than one record may be assigned to a memory location. When this happens, we say that a *collision* occurs. One way to resolve a collision is to assign the first free location following the occupied memory location assigned by the hashing function.

Euclidean Algorithm:

Let $a = bq + r$, where a, b, q and r are integers. Then gcd (a, b) = gcd (b, r).

Proof: If we can show that common divisors of a and b are the same as the common divisors of b and r, we will have shown that gcd (a, b) = gcd (b, r), since both pairs must have the same *greatest* common divisor.

So suppose that d divides both a and b. then it follows that d also divides $a - bq = r$. Hence, any common divisor of a and b is also a common divisor of b and r.

Likewise, suppose that d divides both b and r. then d also divides $bq + r = a$. hence, any common divisor of b and r is also a common divisor of a and b.

Consequently, gcd (a, b) = gcd (b, r).

Ex: *Find* gcd (414, 662) using Euclidean algorithm.

$662 = 414.1 + 248$

$414 = 248.1 + 166$

$248 = 166.1 + 82$

$166 = 82.2 + 2$

$82 = 2.\ 41$

Hence, gcd (414, 662) = 2, since 2 is the last nonzero remainder.

Procedure *gcd* (a,b: positive integers)

```
x : = a
y : = b
while y ≠ 0
begin
      r : = x mod y
      x : =y
      y : = r
end { gcd (a,b) is x}
```

Representation of Integers:

Let b be a positive integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form $n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$

Where k is a nonnegative integer, $a_0, a_1, \dots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

Procedure *base b expansion* (n: positive integer)

```
q : = n
k : = 0
while q ≠ 0
begin
      $a_k$ : = q mod b
      q : = ⌊q/b⌋
      k : = k + 1
end { the base b expansion of n is ($a_{k-1}$ …. $a_1 a_0$)$_b$}
```

Application of Number Theory

Theorem: If a and b are positive integers, then there exist integers s and t such that gcd $(a, b) = sa + tb$.

i.e. gcd (a, b) can be expressed as a *linear combination* with integer coefficients of a and b.

e.g. Express gcd (252, 198) = 18 as a linear combination of 252 and 198.

By the successive division method of Euclidean algorithm

$252 = 1.198 + 54$
$198 = 3.54 + 36$
$54 = 1.36 + 18$
$36 = 2.18$

So,

$18 = 54 - 1.\ 36$
$36 = 198 - 3.54$
$\therefore 18 = 54 - 1.36 = 54 - 1.(\ 198 - 3.54) = 4.54 - 1.198$
$54 = \ 252 - 1.198$
$\therefore 18 = 4.(\ 252 - 1.198) - 1.198 = 4.252 - 5.198$

Linear Congruence

A congruence of the form

$$ax \equiv b\ (\bmod\ m)$$

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence.*

- □ To find all the integers x satisfy this congruence, one method is to find an integer $\bar{a}$ such that $a.\ \bar{a} \equiv 1$ (mod m), if such an integer exists. Such an integer $\bar{a}$ is said to be an *inverse of a modulo m.*

Theorem: If a and $\overset{m}{\cancel{b}}$ are relatively prime integers and $m>1$, then an inverse of a modulo m exists. This inverse is unique modulo m.

Proof: Since gcd (a, m) =1, there are integers s and t such that

$$sa + tm = 1$$

this implies that, $sa + tm \equiv 1\ (\bmod\ m)$

since $tm \equiv 0$ (mod m), it follows that

$$sa \equiv 1\ (\bmod\ m).$$

Consequently, s is the inverse of a modulo m.

Example:

- Find the inverse of 3 modulo 7.

Solution: Since gcd (3, 7) =1, the above theorem tells that an inverse of 3 modulo 7 exists. The Euclidean algorithm ends quickly when we used to find the greatest common divisor of 3 and 7:

$$7 = 2.3 + 1$$

From the equation we can see that,

$$-2.3 + 1.7 = 1.\ (\ sa + tm = 1)$$

This shows that –2 is an inverse of 3 modulo 7.

(The integer congruent to –2 modulo 7 is also an inverse of 3, such as 5, -9, 12, ...)

- Consider the congruence equation

$$6x \equiv 1\ (\bmod\ 33)$$

Since gcd (6, 33) = 3. Thus the equation has no solution.

- consider the congruence equation

$$7x \equiv 1\ (\bmod\ 9)$$

Here gcd (7, 9) = 1; hence the equation has a unique solution. Testing the numbers 0, 1, 2, ..., 8, we find that

$$7\ (4) = 28 \equiv 1\ (\bmod\ 9).$$

Thus $x = 4$ is our unique solution. (The general solution is $4 + 9k$ for $k\ \varepsilon\ \mathbf{Z}$)

- Consider the congruence equation

$$81x \equiv 1 \ (\text{mod } \cancel{280)}\ 256)$$

Here gcd (81, ~~280~~ 256) = 1; hence the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus m = 256 is relatively large. Hence we apply the Euclidean algorithm to a = 81 and m = 256. We find that x_0 = -79 and y_0 = 25 such that $81x_0 + 256y_0 = 1$. This means that x0 = -79 is a solution of the given congruence equation. Adding m=256 to –79, we obtain the unique solution x = 177 between 0 and 255.

Theorem: Suppose a and m are relative prime. The $ax \equiv b$ (mod m) has a unique solution. Moreover, if s is the unique solution to $ax \equiv 1$ (mod m), then $x = bs$ is the unique solution to $ax \equiv b$ (mod m).

- Consider the congruence equation

$$3x = 5 \ (\text{mod } 8)$$

since 3 and 8 are coprime, the equation has a unique solution. Testing the integers 0, 1,...., 7, we find $3\,(7) = 21 \equiv 5$ (mod 8)

Thus x = 7 is the unique solution of the equation.

e.g. Consider the congruence equation

$$3 \quad 33x = 38 \ (\text{mod } 280) \quad \ldots \quad \ldots \quad \text{(i)}$$

since gcd (3~~8~~, 280) = 1, the equation has a unique solution. Testing may not be an efficient way to find the solution here. We apply the Euclidean algorithm to find a solution to

$$33x \equiv 1 \ (\text{mod } 280) \quad \ldots \quad \ldots \quad \text{(ii)}$$

and we find that $33\,(17) + 280\,(-2) = 1$

that means that s = 17 is a solution for equation (ii). Then

$$sb = 17\,(38) = 646$$

is a solution of the original equation (i). Dividing 646 by m = 280, we obtain the remainder

$$x = 86$$

which is the unique solution (i) between 0 and 279.(The general solution is $86 + 280k$ with $k \varepsilon \mathbf{Z}$)

I → 11·27 (P-331 SCS)

Chinese Remainder Theory:

In the first century, the Chinese mathematician Sun-Tsu asked:

> "Is there a positive integer x such that when x is divided by 3 yields a remainder 2, when x is divided by 5 it yields a remainder 4, and when x is divided by 7 it yields a remainder 6?"

The puzzle can be translated into, find the solution of the following congruence equation

$$x \equiv 2 \ (\text{mod } 3)$$
$$x \equiv 4 \ (\text{mod } 5)$$
$$x \equiv 6 \ (\text{mod } 7)$$

Chinese Remainder Theorem

Le~~f~~t $m_1, m_2, \ldots\ldots, m_n$ be pairwise relatively prime positive integers. The system

$$x \equiv a_1 \ (\text{mod } m_1)$$
$$x \equiv a_2 \ (\text{mod } m_2)$$
$$\vdots$$
$$x \equiv a_n \ (\text{mod } m_n)$$

has a unique solution modulo $M = m_1 m_2 \ldots m_n$. (that is, there is a solution x with $0 \le x < M$, and all other solutions are congruent modulo M to this solution).

Solution: Let $M = m_1.m_2.....m_k$. and $M_k = M/m_k$ for $k = 1, 2, \dots, n$.

i.e. $M_1 = M/m_1$, $M_2 = M/m_2$, ..., $M_n = M/m_n$

Let $s_1, s_2, \dots\dots, s_n$ be the solutions, respectively, of the congruence equations

$M_1x \equiv 1 \pmod{m_1}$, $M_2x \equiv 1 \pmod{m_2}$, ... $M_k\, x \equiv 1 \pmod{m_k}$

Then,

$$X = M_1s_1b_1 + M_2s_2b_2 + \dots + M_ns_nb_n$$

is the solution of the system.

Here $M = 3.5.7 = 105$
$M_1 = 105/3 = 35$
$M_2 = 105/5 = 21$
$M_3 = 105/7 = 15$

Now we seek the solution to the equation

$35.x \equiv 1 \pmod 3$
$21.x \equiv 1 \pmod 5$
$15\, x \equiv 1 \pmod 7$

reducing 35 modulo 3, 21 modulo 5, 15 modulo 7, we have /using inverse

$2x \equiv 1 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 7$

the solution of these three equations are

$s_1 = 2, s_2 = 1, s_3 = 1$

$\therefore \quad X = 35.2.2 + 21.1.4 + 15.1.6$
$= 314$

dividing this solution by modulus $M = 105$, we obtain $x = 104$ which is the unique solution between 0 and 104.

□ The integers $a_1, a_2, \dots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ where $1 \le i < j \le n$.

Pseudoprimes: There are composite integers n such that $2^{n-1} \equiv 1 \pmod n$. Such integers are called pseudoprimes.

e.g. The integer 341 is a pseudoprime since it is composite (341=11. 31) and $2^{340} \equiv 1 \pmod{341}$.

□ Ancient Chinese mathematicians believed that n was prime if and only if $2^{n-1} \equiv 1 \pmod n$.

□ But they were partially correct. The great French mathematician Fermat showed that the congruence holds when n is prime.

Fermat's Little Theorem:

If p is prime and a is an integer not divisible by p then $a^{p-1} \equiv 1 \pmod p$.

Furthermore, for every integer a we have $a^p \equiv a \pmod p$.

□ Although the ancient Chinese were wrong, pseudoprimes are relatively rare.