Unit-3 Number Theory (4.1 to 4.3.7)

In this unit, we will develop some concept based on the notation of divisibility. The division of an integer by a positive integer produce a quotient and a remainder working with these remainder lead to moduler arithmetic which plays a import-ant rule in mathematics and which is used throughout computer science.

→ Division

Defination 1: If a and b are intergers with $a \neq 0$, we say that a divides b if their is a integer c such that $b = ac$ when a divides b we say that a is a factor or divisor of b, and that b is a multiple of a. The notation $a|b$ denotes that a divides b. We write $a \nmid b$, we say that a does not divide b.

Example①: Determine whether $3 \nmid 7$ and whether $3|12$

Sol^n: We see that 3 does not divide 7 because 7 divide 3 is not an integer. On the other hand 3 divide 12 because $12/3 = 4$ is an integer.

Example ②: Let n and d be positive integers how many positive integer not exceeding n is not divisible by d.

Sol^n: The positive integer divisible by d are all the integer of the form dK, where K is a positive integer. Therefore the positive integer divisible by d that do not exceed n equals the no of integer K with $0 < dK \leq n$ or with $0 < K \leq \frac{n}{d}$

Therefore their are $\lfloor n/d \rfloor$ positive integer not exceeding n that are divisible by d.

→ Theorem

- Let a, b and c where $a \neq 0$.
  (a) If $a|b$ and $a|c$ then $a|(b+c)$
  (b) If $a|b$ and $a|bc$ ∀ integer c
  (c) If $a|b$ and $b|c$ then $a|c$
  ~~(d) If~~
- If a, b and c where $a \neq 0$ such that $a|b$ and $a|c$ then $a|(mb+nc)$ where m and n are integers.

→ The division algorithm

Let **a** be an integer and **d** a positive integer, their is a unique integer q and r with $0 \leq r < d$ such that $\boxed{a = dq + r}$

a = divident
d = divisor
q = quotient
r = remainder

$\boxed{9 = 2 \times 4 + 1}$

$2 \,)\, 9 \,($ 4
8
1

In the Equality given in division algorithm, d is called divisor, a is called divident, q called quotient, r is called remainder. This notation is used to express quotient and remainder

$\boxed{q = a \text{ div } b}$ Note: Both a div b and a mod d
$\boxed{r = a \text{ mod } d}$ for a fix d are function on the set of integer. Additionally, when a is an integer and d is a positive integer then we have $a \text{ div } b = \lfloor a/b \rfloor$, $a \text{ mod } d = a - d$

Example: What are the quotient and remainder when 101 divided by 11.

$$101 = 11 \cdot 9 + 2$$
$$a = d\,q + r$$

$$\begin{array}{r} 9 \\ 11\overline{)101} \\ 99 \\ \hline 2 \end{array}$$

$q = 101 \text{ div } 11$ $\quad$ $r = 101 \text{ mod } 11$

$\boxed{q = 9}$ $\quad$ $\boxed{r = 2}$

Example: What are the quotient and remainder when -11 divide by 3.

$$-11 = 3 \cdot (-4) + 1$$

because $r = -2$, $0 \le r < 3$

$q = -11 \text{ div } 3$ $\quad$ $r = -11 \text{ mod } 3$

$\boxed{q = -4}$ $\quad$ $\boxed{r = 1}$

→ Modular Arithmetic

If a and b are integer 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. If ~~this is~~ $a \equiv b \pmod m$ is congruent and that m is its modulus (plural moduli) If a and b are not ~~contra~~ congruent modulo m then $a \not\equiv b \pmod m$

Note: If a and b are integer and let m be a positive integer then $a \equiv b \pmod m$ if and only if $a \text{ mod } m = b \text{ mod } m$.

Q Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

$a \equiv b \bmod (m)$

$17 \equiv 5 \bmod (6)$ ~~then 17-5=12~~

~~12 is divisible by 6~~.

$6 \text{ div } 17-5 = 6 \mid 12$

Therefore, we see that $17 \equiv 5 \bmod (6)$. However because $24-14=10$ is not divisible by 6

Therefore we see that $24 \not\equiv 14 \bmod (6)$

Theorem: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer K such that $\boxed{a = b + Km}$.

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

Example: Because $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, it follow this Theorem.

then $7+11 \equiv 2+1 \pmod 5$

$18 \equiv 3 \pmod 5$ and

$5 \mid (18-3) = 5 \mid 15 = 3$

$7 \cdot 11 \equiv 2 \cdot 1 \pmod 5$

$77 \equiv 2 \pmod 5$

$5 \mid (77-2) = \frac{5}{75} = 15$

~~Theorem~~:

Let m be a positive integer and let a and b be integer then,

$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

and

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

~~Q Find the~~ value of $(19^3 \bmod 31)^4 \bmod 23$

$19^3 \bmod 31$

$19^3 = 6859$

$6859 = 221 \cdot 31 + 8$

$6859 \bmod 31 = 8$

$\Rightarrow 8^4 \bmod 23$

$8^4 = 4094 = \cancel{4096}$

$4094 = 178 \cdot 23 + 2$

$4094 \bmod 23 = 2$

Arithmetic modulo m

We can define arithmetic operation on Z_m, the set of non-negative integer less than m that is, the set $\{0, 1, \ldots, m-1\}$.
In particular we define addition of these integers denoted by $+_m$ by

$$\boxed{a +_m b = (a+b) \bmod m}$$

Where addition on right hand side of this Eq^n is ordinary addition integer and we define multiplication of these integers denoted by $\cdot_m$ by

$$\boxed{a \cdot_m b = (a \cdot b) \bmod m}$$

where multiplication of right hand side is ordinary multiplication of integers.
The operation $+_m$, $\cdot_m$ are called addition & multiplication modulo m. and when we use these operations we said we doing arithmetic modulo m.

Example Use the defination of addition & multiplication in Z_m to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

$7 +_{11} 9 = (7+9) \bmod 11$
$= 16 \bmod 11 = 5$

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11$
$= 63 \bmod 11 = 8$

The operation $+m$ and $\cdot m$ satisfy many of the same properties of ordinary addion and multiplication of integers.
Associative, closures, commutative, identity element additive inverse and distributive all these properties hold in arithmetic modulo m.

→ Representation of Integers

Theorem: Let b be an integer greater than 1. then if n is a positive integer, it can be Express uniquely in the form.

$n = a_k b^k + a_k b^{k-1} + \cdots + a_1 b + a_0$

where k is a non-negative integer, $a_0, a_1, \ldots a_k$ are nonnegative integer less than b, and $a_k \neq 0$

Ex: What is the decimal Expansion of the integer that has $(101011111)_2$ as its binary Expansion

$(101011111)_2 = 1 \times 2^8 + 0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4$
$1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 351$

Binary Expansion
octal & hexidecimal Expansion:
... the most important base are 2, 8, and 16

Base 8 Expansion are called Octal Expansion
Base 2 ,, Binary Expansion
Base 16 ,, hexadecimal Expansion

Q what is the decimal expansion of no. $(7016)_8$ with octal Expansion:

$$(7016)_8 = 7 \times 8^3 + 0 \times 8^2 + 1 \times 8^1 + 6 \times 8^0$$
$$= 3584 + 0 + 8 + 6$$
$$= 3598$$

→ **Digit Requirements for hexadecimal Expansion**

16 different digit are required for hexadecimal Expansion:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Ex: what is the decimal Expansion of a no. $(2AE0B)$ → ~~(2 10 14 0 11)~~

$$= 2 \times 16^4 + 10 \times 16^3 + 14 \times 16^2 + 0 \times 16^1 + 11 \times 16^0$$
$$= 175627$$

→ **Bit Representation of hexadecimal digits**

Each hexadecimal digit can be using four bits. for Ex:, we can see that

$$(\underbrace{1110}\ \underbrace{0101})_2 = (E5)_{16}$$

$\underset{2^3\,2^2\,2^1\,2^0}{1110} = 14 = E$

$\underset{2^3\,2^2\,2^1\,2^0}{0101} = 5$

$(\underbrace{1110}\ \underbrace{0101})_2 \rightarrow (71)_8$

~~$1110 = 4$~~

~~$001 = 1$~~

$101 = 5$
100
011

0000
1001
2 000
3 011
4 100
5 101
6 1 00
7 111

2

2·14 + 6
111

$f(a,b) = f_X(a) \cdot f_Y(b) \quad \forall a, b$

When X and Y

<u>Discrete</u>

~~When X and Y~~

→ <u>Base conversion</u>

We will now describe an algorithm for constructing the base b, Expansion of an integer n. Firstly divide n by b. to obtain a quotient and remainder that is, $n = b q_0 + a_0$; $0 \le a_0 < b$
The remainder a_0 is the right most digit in the base b Expansion of n. Next divide q_0 by b to obtain $q_0 = b q_1 + a_1$; $0 \le a_1 < b$
In this a_1 is the second digit from the right in the base b. Expansion of n. continuing this process dividing quotient by b, obtaining additional base b with its as a remainder. This process terminate when quotient is zero. So it produce the base b digit of n from the right to the left.

Q Find the octal Expansion of $(12345)_{10}$

First divide 12345 by 8 to obtain

$12345 = 8 \cdot 1543 + 1$

$1543 = 8 \cdot 192 + 7$

$192 = 8 \cdot 24 + 0$

$24 = 8 \cdot 3 + 0$

$3 = 8 \cdot 0 + 3$

The successive remainder that we have found 1, 7, 0, 0, and 3 are the digit from right to the left of 12345 in base 8. Therefore

Assign

Q Find the hexadecimal Expansion of $(177130)_{10}$

First divide 177130 by 16 to obtain

$177130 = 16 \cdot 11070 + 10$

$11070 = 16 \cdot 691 + 14$ $\quad$ $(177130)_{10} = (453A)_{16}$

$691 = 16 \cdot 43 + 3$

$43 = 16 \cdot 2 + 11$ $\quad$ $(177130)_{10} \rightarrow (2B3EA)_{16}$

$2 = 16 \cdot 0 + 2$

Assign

Q Find the Binary Expansion of $(241)_{10}$

$241 = 120 \times 2 + 1$
$120 = 60 \times 2 + 0$
$60 = 30 \times 2 + 0$
$30 = 15 \times 2 + 0$
$15 = 7 \times 2 + 1$
$7 = 3 \times 2 + 1$
$3 = 1 \times 2 + 1$
$1 = 0 \times 2 + 1$

Assign

Q Find the octal and hexidecimal Expansion of $(11\ 1110\ 1011\ 1100)_2$ & Binary Expansion of $(765)_8$ and $(A8D)_{16}$

$(011\ 111\ 010\ 111\ 100)_2 \rightarrow$

→ Algorithm of Integer operation

The algorithm for performing operation with integer using $a = (a_{n-1}\ a_{n-2} - - a_1\ a_0)_2$, $b = (b_{n-1}\ b_{n-2} - - b_1\ b_0)_2$ are extremely important in computer arithmetic. In this section we all describe the algorithm for addition & multiplication of two integer ~~Expon~~ Expressed in binary notation.

Suppose that binary operations of a & b are
$a = (a_{n-1}\ a_{n-2} - - a_1, a_0)$, $b = (b_{n-1}\ b_{n-2} - - b_1, b_0)_2$
where a & b each have n bits (putting bits equal to 0, at the begining of one of these Expansions if necessary).

Rule of addition

$0+0=0$
$0+1=1$
$1+0=1$
$1+1=10$

→ Addition Algorithm

This algorithm ~~will use~~ processed by adding pair of binary digit together with carries when they occur to compute the sum of two binary integers. To add a & b, just add their right most bits this give ~~a_0+b_0~~ $\boxed{a_0+b_0 = C_0 \times 2 + S_0}$, where S_0 is the right most bit in the binary Expansion of $a+b$ and C_0 is the carry which is either 0 or 1. then at the next pair of bit & the carry $\boxed{a_1+b_1+c_0 = c_1 \times 2 + S_1}$ where S_1 is the next bit (from the right) in the binary Expansion of $a+b$ and c_1 is the carry. Continue this process, adding the corresponding bits in the two binary expansion of the carry to determined the next bit from the right in the binary expansion of $a+b$.

At the last stage add a_{n-1}, b_{n-1} and C_{n-2} to obtain $\boxed{C_{n-1} \times 2 + S_{n-1}.}$ the leading bit of the sum is $S_n = C_{n-1}$. This process produc the binary Expansion of the sum namely

$a+b = (S_n\, S_{n-1}\, S_{n-2} \cdots S_1 S_0)_2$

Q Add $a = (\underset{a_3}{1}\underset{a_2}{1}\underset{a_1}{1}\underset{a_0}{0})_2$ and $b = (\underset{b_3}{1}\underset{b_2}{0}\underset{b_1}{1}\underset{b_0}{1})_2$

step 1. $a_0 + b_0 = 0 + 1 = 2 \times 0 + 1 = 1$

So, that

$C_0 = 0$ and $S_0 = 1$ then; because

step 2 $a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \times 2 + 0.$

$\therefore C_1 = 1$ and $S_1 = 0$

~~Step~~ Step 3 $a_2 + b_2 + c_1 = 1 + 0 + 1 =$ [redacted] $\times 2 + 0$

$\therefore c_2 = 0$ and $S_2 = 1$

~~Step~~ Step 4 $a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \times 2 + 1$

$\therefore c_3 = 1$ & $S_3 = 1$

This means

~~s~~ $S_4 = c_3 = 1$

$\therefore s = a + b = (11001)_2$

→ ~~Multiplication algorit~~

Q How many addition of bits are required to add two integer ~~side~~ by addition algorithm with n bits in their binary representation.

Ans Two integers are added by successively adding pairs of bits when it occur a carry. Adding each pair of bits & the carry ~~required the~~ two addition of bits. ∴ the total no. of addition of bits used is less than twice the no. of bits expansion. The no. of addition of bits used by algorithm to add n-bits of integer $O(n)$.

→ Multiplication algorithm

multiplication rule

$0 \times 0 = 0$

$0 \times 1 = 0$

$1 \times 0 = 0$

$1 \times 1 = 1$

$$
\begin{array}{r}
110 \\
\times\ 101 \\
\hline
110 \\
000 \\
110 \\
\hline
11110
\end{array}
$$

the multiplication of n-bit integers a & b by the algorithm we see that

$a \times b = a(b_0 2^0 + b_1 2^1 + \dots + b_{n-1} 2^{n-1})$

$= a(b_0 2^0) + a(b_1 2^1) + \dots + a(b_{n-1} 2^{n-1})$

{Using Distributive law}

We can compute $a \times b$ or ab, using the above eqⁿ we first note that $ab_j = a$ if $b_j = 1$ and $ab_j = 0$ if $b_j = 0$. Each time we multiply a term by two then we shift its binary expansion one place to the left and add 0 at the tail of of the expansion.

Therefore, we can obtain $(ab_j)2^j$ by shifting the binary expansion of ab_j j places to the left, adding j zero bits at the tail end of this binary expansion. Finally, we obtain ab by adding the n integers $ab_j 2^j$; $j = 0, 1, 2 \dots$,

{n = no of bits}

Q Find the product of $a = (\underset{a_2}{1}\underset{a_1}{1}\underset{a_0}{0})_2$ and $b = (\underset{b_2}{1}\underset{b_1}{0}\underset{b_0}{1})_2$

n=3

$ab_0 \times 2^0 = (110)_2 \times 1 \times 2^0 = (110)_2$

$ab_1 \times 2^1 = (110)_2 \times 0 \times 2^1 = (0000)_2$ shift

$ab_2 \times 2^2 = (110)_2 \times 1 \times 2^2 = (11000)_2$ shift

To find the product the product add $(110)_2$, $(0000)_2$ & $(11000)_2$

So,

$$\begin{array}{r} 110 \\ 0000 \\ 11000 \\ \hline 11110 \\ \hline \end{array}$$

$\therefore ab = (11110)_2$

→ Modular Exponentiation

To avoid the large amount of memory. To multiplied the huge no. ~~to~~ and find the modulus out of it. We use fast modular ~~Expansion~~ Exponentiation algorithm. In this algorithm, we use the binary Expansion of n say $n = (a_{k-1} \cdots a_1 a_0)_2$, to compute b^n. First note that $b^n = b^{a_{k-1} \times 2^{k-1} + \cdots + a_1 \times 2} \times b^{a_0}$.

This show that to compute b^n we need only compute the value of b, $b \cdot b^2$, $(b^2)^2 = b^4$, $(b^4)^2 = b^8$, ..., b^{2^k}. Once we have these values we multiplied the terms b^{2^i} in this list where $a_j = 1$ (for efficiency and reduce space requirements after multiplying by each term we reduce the result modulo m, this gives us b^n)

For Example: To compute 3^{11}

$11 = (1011)_2$

$2^3\ 2^2\ 2^1\ 2^0$

$8 + 0 + 2 + 1 = 11$

$3^{11} = 3^8\, 3^2\, 3$

$= 6561 \times 9 \times 3$

$= 177,147$

Q. Find $3^{644} \bmod 645$

→ Prime and Greatest Common Divisor

• **Prime**: An integer 'p' greatest than 1 is called prime if the only positive factor of p is 1 and p. The positive integer not greater than 1, and is not prime is called composite.

• **Fundamental theorem of arithmetic**

Every integer greater than 1 can be written uniquely as a prime or as a product of 2 and more prime where the prime factors are written in the order of non-decreasing i.e.

Example: Q The prime factorization of 100, 641, 999 and 1024.

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$641 = 641$

$999 = 3 \times 3 \times 3 \times 37 = 3^3 \times 37$

$1024 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^{10}$

→ Trivial Division

If n is the composite integer then n has prime divisor less than or equal to $\sqrt{n}$.

Q Show that 101 is prime.

Ans The only prime not exceeding $\sqrt{101}$, are 2, 3, 5 and 7 because 101 is not divisible by 2, 3, 5 and 7. Therefore ~~then~~ it follow 101 is prime.

Assign

Q Find prime factorization of 7007

→ The Prime number Theorem

The ratio of $\pi(n)$, the primes not exceeding n and $\frac{x}{\ln(n)}$ approaches 1 as n grows without bound. Here ln is the natural log.

→ Twin prime

Twin prime are the prime that differ by 2, 3 and 5, 5 and 7, ... 4967 & 4969

→ The Twin prime Conjecture

→ conjectures and open problems on prime

Notes by Andrew Ng

• The Twin prime Conjucture

The Twin prime conjucture states that there are infinetely many twin prime. The strongest result proove concerning twin primes is that their are infinitely many pair $p, p+2$ where p is prime and $p+2$ is prime or the product of two primes.

→ Gretest Common Divisor (GCD)

Let a and b be integers not both zero. The largest integer d such that $d|a$ and $d|b$, and D called the GCD and denoted by $gcd(a,b)$

Q What is ~~greatest~~ GCD of 24 & 36

Solⁿ $gcd(24, 36) = 12$

Assign

Q What is GCD of 17 and 22. Is this relatively prime or not.

→ Relatively Prime

The integer a & b are relatively prime if their gcd is 1.

Q Determine whether 10, 17 and 21 are pair wise relatively prime and whether the integer 10, 19 and 24 are pair wise relatively prime.

Defination: The integer $a_1, a_2 \ldots a_n$ are pair wise relatively prime if $gcd(a_i, a_j) = 1$ whether $i, 1 \leq i < j \leq n$.

4. $gcd(10, 17) = 1$
$gcd(17, 21) = 1$
$gcd(10, 21) = 1$
So, 10, 17, 21 are pair wise relatively prime

$gcd(10, 19) = 1$
$gcd(19, 24) = 1$
$gcd(19, 24) = 2$
So, 10, 19, 24 are not pair wise relatively prime

• Another way to find the GCD of two positive integers is to used the prime factorization of these integers.

Suppose that prime factorization of the positive integer a & b are $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$, where each exponent is a non-negative integer & where all primes occuring the prime factorization of either a & b are including in both factorization with the zero exponent if necessary then gcd of a & b is given by

$$gcd(a,b) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)} \ldots p_n^{min(a_n, b_n)}$$

§ Because Find the prime factorization of 120 and 500.

$120 = 2^3 \times 3 \times 5$
$500 = 2^2 \times 5^3$

$gcd(120, 500) = 2^{min(2,3)} \times 3^{min(0,1)} \times 5^{min(1,3)}$
$= 2^2 \times 3^0 \times 5$
$= 20$ Ans

§ → Prime factorization can also find least common multiple (LCM).
The LCM of positive integers a & b is the smallest positive integer is divisible by both a & b. It is denoted by $lcm(a,b)$

$$lcm(a,b) = p_1^{max(a_1, b_1)} \times p_2^{max(a_2, b_2)} \times \ldots p_n^{max(a_n, b_n)}$$

Q what is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

$$lcm(a,b) = 2^{max(3,4)} \cdot 3^{max(5,3)} \cdot 7^{max(2,0)}$$
$$= 2^4 \cdot 3^5 \cdot 7^2.$$

→ Relationship b/w gcd & lcm.

$$\boxed{ab = gcd(a,b) \times lcm(a,b)}$$

→ Euclid Algorithm

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

Imp. Assign

Q Find the greatest common divisor 414 & 662 using Euclid Algorithm.