Chapter-1

Some Topics in Elementary Number Theory:

(1) Time Estimates for doing arithmetic:

A non negative integer n written to the base b is a notation for n of the form $(d_{k-1}\, d_{k-2} \cdots d_1\, d_0)_b$, where the d's are digits.

This notation means that:

$$n = d_{k-1} \cdot b^{k-1} + d_{k-2} b^{k-2} + \cdots d_1 b + d_0.$$

if $d_{k-1} \neq 0$, then n is a k digit base b number.

Remark (i) Fractions can also be expanded in any base, i.e they can be represented in the form
$(d_{k-1}\, d_{k-2} \cdots d_1\, d_0\, d_{-1}\, d_{-2} \cdots)_b$

(ii) When base > 10 it is customary to use letters for the digits beyond 9. We can also use letters for all the digits.

Ex-1 (a) $(11001001)_2 = 201$

(b) When base $= 26$, use letters A-Z for the digits 0-25, then,

$$(BAD)_{26} = 26^2 \times 1 + 26^1 \times 0 + 26^0 \times 3 = 679$$

Ex-2 Multiply 160 and 199 in base 7.

Soln

~~160 → (160)7~~ ~~1×7²+6×7¹+0×7⁰~~

~~199 → (199)7~~

$(160)_{10} \rightarrow (316)_7$

$(199)_{10} \rightarrow (403)_7$

$$\begin{array}{r} {}^{1}{}^{2} \\ 3\,1^{3}\,6_7 \\ \times\ 4\,0\,3_7 \\ \hline 1\,2\,5\,4 \\ 1\,6\,0\,3\,0 \\ \hline 1\,6\,1\,5\,5\,4 \end{array}$$

18 = 7×2+4

3 = 7×0+3

9 = 7×1+2

24 = 7×3+3

14 = 7×0+4

12 = 7×1+5

7 = 7×1+0

Ex. Divide $(1100\,1001)_2$ by $(100\,111)_2$

Soln

$$\begin{array}{r|l} 100111 \overline{)\,1100\,1001} & 101 \\ -100\,111 & \\ \hline 101\,101 & \\ 100\,111 & \\ \hline 110 & \end{array}$$

110
100111

Ex-5. Convert $\pi = 3.1415926$ to the base 2 and to the base 26.

Sol^n (a) $(3.1415)_{10} = (\quad)_2$

2 | 3		
2 | 1	1	↑
0	1	

$0.1415 \times 2 = 0.283 \quad 0$
$0.283 \times 2 = 0.566 \quad 0$
$0.566 \times 2 = 1.132 \quad 1$
$0.132 \times 2 = 0.264 \quad 0$ ↓
0.264×2

$= (11.0010)_2$ Ans

(b) $(3.1415)_{10} = (\quad)_{26}$.

26 | 3	3	↑
0		

$0.1415 \times 26 = 3.679 \quad 3$
$0.679 \times 26 = 17.654 \quad 17$
$0.654 \times 26 = 17.004 \quad 17$ ↓

$(3.3RS)_{26}$ Ans.

Number of digits :-

An integer n satisfying $b^{k-1} \leq n < b^k$ has k digits to the base b.

So, no. of digits $= [\log_b n] + 1 = \left[\frac{\log n}{\log b}\right] + 1$.

The amount of time a computer takes to perform a task is essentially proportional to the number of bit operation.

Time (multiply integer k bits long by integer $< kl$ l bits long)

Ex-6 Find an upper bound for the number of bit operations required to compute $n!$.

Sol" Step-1 First we multiply 2 by 3, then this result is multiplied by 4, then the result is multiplied by 5 and so on.

* At $(j-1)$th step we are multiplying $j!$ by $(j+1)$. Hence we have $(n-2)$ steps.

* To find the no of bits in the product, we use the fact that the no of digits in the product of two numbers is either the sum of the no of digits in each factor or 1 less than the sum.

* From this, the product of n k-bit integer will have at most nk bits.

* If n is a k bit Integer this implies that every integer less than n has atmost k bits and $n!$ has at most (nk) bits.

* In Each $(n-2)$ multiplication, we are multiplying an integer with ~~k bits~~ at most k bits by an integer with atmost nk bits. This requires nk^2 bits operations at most.

We are repeating this for $(n-2)$ times, so,

total bits operation $= nk^2(n-2)$

$= n(n-2)k^2$

putting the value of k,

$n(n-2)(1+\log_b n)^2$

$\simeq n^2(\log n)^2$

Ex.7 find an upper bound for the no of bit op^n required to multiply a polynomial $\sum a_i x^i$ of degree $\leq n_1$ and a polynomial $\sum b_j x^j$ of degree $\leq n_2$ whose coefficients are positive integers $\leq m$. Let $n_2 \leq n_1$.

Soln $\sum_{i+j=v} a_i b_j \longrightarrow$ coefficient of x^v in the product polynomial.

$(0 \leq v \leq n_1+n_2)$.

* this requires at most n_2+1 multiplication
n_2 addition.

* The numbers being multiplied are bounded by m, and the no being added are added at most m^2.

Since we have to add n_2 numbers, then the bound should be atmost $n_2 m^2$.

Thus in computing the coeff of x^v the no of bit op^n req. is at most,

$$(n_2+1)(\log_2 m+1)^2 + n_2(\log_2(n_2 m^2)+1).$$

Since there are n_1+n_2+1 values, our time estimate for the polynomial mult^n is.

$$(n_1+n_2+1)\left((n_2+1)(\log_2 m+1)^2 + n_2(\log_2(n_2 m^2)+1)\right).$$

* Time (subtract k bit from l-bit) $\leq \max(k,l)$

* Time (divide k bit by l-bit) $\leq kl$.

The big-O Notation:-

Suppose that $f(n)$ and $g(n)$ are fn of the positive integers n which take positive values for all n. Then, we say,

$f(n) = O(g(n))$ if there exists a constant C such that $f(n)$ is always less than $C \cdot g(n)$.

for ex:- $2n^2 + 3n - 3 = O(n^2)$ this is always less than $O(3n^2)$.

Ex-10 Estimate the time required to convert a K bit Integer to its representation in the base 10.

Sol" Let 'n' be a K bit Integer written in binary.

We will divide n by 10:

Let $n = (1010)_2 = 10$.

Then, the remainder will be one of the digit 0, 1, 10, 11, 100, 101, 110, 111, 1000 or 1001 - this will be ones digit do.

Now we will replace n by the quotient and repeat the process.

The process will be repeated the no of times as the no of digits in n. i.e,

$$\left[\frac{\log n}{\log 10}\right] + 1 = O(k).$$

Now, we have to do ~~approx~~ $O(k)$ divisions, each requiring $O(4k)$ operation as dividing a number with at most K bits by 4 bit number)

$O(4K)$ is same as $O(K)$.

So the total no. of bit operations are = $O(K) \cdot O(K)$

$= O(K^2)$.

and since $K = \log n$.

> Time (convert n to decimal) = $O(\log^2 n)$.

Q-11. Estimate the time required to convert a K bit Integer n to its representation in the base b.

Soln: Let b is a l bit Integer.
and given n is a K bit integer.

Now, division of K bit Integer by l bit Integer will take $O(Kl)$ operations. — (1)

* Now the no of base b. digits in n is $O\left(\frac{K}{l}\right)$. — (2)

Total no of bit operations required

$= O(K/l) * O(Kl) = O(K^2)$.

Estimate for the conversion time does not depend upon the base to which we are converting.

* This is because the greater time required to find each digit is offset by the fact that there are fewer digits to be found.

(II) Divisibility and Euclidean algorithm :-

* **divisors and divisibility :-** Given integers a and b, we say a divides b. ($a|b$) if there exist an integer d such that $b = ad$.

* Every Integer $b > 1$ has at least two positive divisors 1 and b.

Properties of divisibility :-

(i) If $a|b$ and c is any Integer, then $a|bc$.
(ii) If $a|b$ and $b|c$ then $a|c$.
(iii) If $a|b$ and $a|c$, then $a|b \pm c$

* The fundamental theorem of arithmetic says that any natural number n can be written uniquely as a product of prime numbers.

Ex $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.

(iv) If a prime no p divides ab, then either $p|a$ or $p|b$.
(v) If $m|a$ and $n|a$ and if m and n have no divisors greater than 1 in common, then $mn|a$.

Note:- The number of possible divisors is thus the product of no of possibilities for each prime power, which is $(\alpha+1)$.

That is, a no $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}$ has

$(\alpha_1+1)(\alpha_2+1) \cdots (\alpha_r+1)$ different divisors

GCD of two numbers:-

Given two integer a and b, the gcd of a and b, denoted gcd(a,b) is the largest integer d dividing both a and b.

* $lcm(a,b) = |ab| / gcd(a,b)$

The euclidean theorem:-

To find gcd(a,b) where a>b,

(1) We first divide a by b and write down the quotient q_1 and the remainder r_1

$$a = q_1 b + r_1 \quad \text{---} (1).$$

(2) Next we perform a second division with b playing the role of a and r_1 playing the role of b.

$$b = q_2 r_1 + r_2 \quad \text{---} (2)$$

We continue this till we finally obtain a remainder that divides the previous remainder. That final non-zero remainder is the gcd(a,b).

Ex-1. gcd(1547,560)

Soln

$$1547 = 560 \times 2 + 427$$
$$560 = 1 \cdot 427 + 133$$
$$427 = 3 \cdot 133 + 28$$
$$133 = 4 \cdot 28 + 21$$
$$23 = 1 \cdot 21 + 7.$$

Since 7|21, we are done gcd(1547,560) = 7.

* $GCD(a,b) = GCD(b, a\%b)$

* The euclidean algorithm always gives the greatest common divisor in a finite no. of steps.

Time (finding gcd(a,b) by euclidean algo.) = $O(\log^3 a)$.

Note:-

Let $d = gcd(a,b)$, where $a > b$ then there exist integers u and v such that $d = ua + vb$.

In other words, the gcd of two no. can be expressed as a linear combination of no. with integer coefficients.

* a, b are said to be relatively prime if gcd(a,b) = 1. i.e they have no common divisor greater than 1.

Ex. gcd(1547, 560) = 7

a) $21 * 1547 - 58 * 560 = 7$

(iii) Congruences :-

Given three integers a, b and m we say that "a is congruent to b modulo m" and write $a \equiv b \bmod m$, if diff. $a-b$ is divisible by m.
m is called modulus of the congruence.

Properties :-

(a) $a \equiv a \bmod m$

(b) $a \equiv b \bmod m$ if and only if $b \equiv a \bmod m$.

(c) if $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$

(d) if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then,

$a \pm c \equiv b \pm d \bmod m$ and $ac \equiv bd \bmod m$.

(e) if $a \equiv b \bmod m$, then $a \equiv b \bmod d$ for any divisor $d | m$.

(f) if $a \equiv b \bmod m$, $a \equiv b \bmod n$, and m and n are relatively primes, then, $a \equiv b \bmod mn$.

Note :- If we want to solve a linear congruence $ax \equiv b \bmod m$ where $0 \leq a, b < m$.

(a) if $\gcd(a, m) = 1$, then there is a solution x_0 which can be found in $O(\log^3 m)$ bit operations. and all solutions are of the form $x = x_0 + tmn$.

$ax - b = rm$.

$ax - rm = b$

(b) if $\gcd(a, m) = d$, there exit a solution if and only if $d | b$ in that case our congruence is equivalent to the congruence $a'x \equiv b' \bmod m'$

where, $a' = a/d$, $b' = b/d$ and $m' = m/d$.

Fermat's little theorem:- Let p be a prime. Any integer a satisfies $a^p \equiv a \bmod p$ and any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \bmod p$.

Chinese remainder theorem:-

Suppose we want to solve a system of linear congruence.

$$x = a_1 \bmod m_1,$$
$$x = a_2 \bmod m_2$$
$$\vdots$$
$$x = a_r \bmod m_r.$$

Suppose each type of moduli is relatively prime
$\gcd(m_i, m_j) = 1$.
then there exists a simultaneous solution x to all the congruences.

4.) Some applications to factoring :-

* for any Integer b and any positive integer n, $b^n - 1$ is divisible by $b-1$ with quotient $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$.

$$(b^n - 1) = (b-1)(b^{n-1} + b^{n-2} + \cdots b^2 + b + 1)$$
$$= (b^n + b^{n-1} + \cdots b^3 + b^2 + b) - (b^{n-1} + b^{n-2} + \cdots b + 1)$$
$$= (b^n - 1)$$

* for any Integer b and any positive integer m and n, we have $b^{mn} - 1 = (b^m - 1)(b^{m(n-1)} + b^{m(n-2)} + \cdots b^m + 1)$.

⇒ Lets replace b with b^m in previous eqⁿ

$$(b^m)^n - 1 = (b^m - 1)((b^m)^{n-1} + (b^m)^{n-2} + \cdots (b^m)^2 + (b^m) + 1)$$
$$= b^{mn} - 1 .$$

* If b is prime to m, and a and c are positive integers if $b^a \equiv 1 \bmod m$ and $b^c \equiv 1 \bmod m$ and if $d = \gcd(a, c)$ then,

$$\boxed{b^d \equiv 1 \bmod m}$$

* if p is a prime dividing $b^n - 1$, then either

(a) $p \mid b^d - 1$ for some proper divisor d of n.

(b) $p \equiv 1 \bmod n$ if $p > 2$ and n is odd,

$$p \equiv 1 \bmod 2n$$