UNIT-III

Divisibility Theory and Canonical Decompositions

Division Algorithm: 1

Let a be any integer and b be a positive integer. Then there exist unique integers q and r such that $a = bq + r$, $0 \leq r < b$.

Proof:

Existence part:

Let $S = \{a - bn : n \in \mathbb{Z} \text{ and } a - bn \geq 0\}$

Then, first we prove that S is non-empty.

Case (i): Let $a \geq 0$.

Then $a - b(0) = a \geq 0$ with $0 \in \mathbb{Z}$.

$\Rightarrow a \in S$

Hence S is non-empty.

Case (ii) Let $a < 0$

Since b is a positive integer $\Rightarrow b \in \mathbb{Z}^+$, $b \geq 1$.

ie, $b \geq 1$

$\Rightarrow ab \leq a$ $[\because a < 0]$

$\Rightarrow -ba \geq -a$

$\Rightarrow a - ba \geq 0$ with $a \in \mathbb{Z}$.

$\Rightarrow a - ba \in S$

In both cases, S contains atleast one element.

$\therefore$ S is non-empty subset of W

$\therefore$ By well-ordering principle,

$\Rightarrow$ S contains a least element r,

Since $r \in S$, an integer q exists such that,

$$r = a - bq \text{ , where } r \geq 0.$$

$$\Rightarrow a = b.q + r \text{ , and } r \geq 0.$$

To show that $r < b$.

To prove this by contradiction.

Assume that $r \geq b$, ie, $r - b \geq 0$

$$\text{But } r - b = (a - bq) - b$$
$$= a - bq - b$$
$$= a - b(q+1).$$

is of the form $(a - bn)$ and ≥ 0.

$$\Rightarrow a - b(q+1) \in S$$
$$\Rightarrow r - b \in S$$

Since $b > 0$, $r - b < r$

Hence, $r - b$ is smaller than r and in S.

This contradicts the least nature of r.

$\therefore$ $r < b$

Hence, there exist integers q and r such that

$$a = bq + r, \; 0 \leq r < b.$$

Well-ordering Princi…

Any non-empty subs…

of natural numbe…

has a smallest elem…

$S = \{\underline{1}, 2, 3 \ldots$

$r = 1$

$1 - 3 < 1$

$-2 < 1$

Scanned with CamScanner

Uniqueness part:

To prove that the integers q and r are unique.

Assume $a = bq + r, \ 0 \le r < b. \rightarrow ①$

and $a = bq' + r', \ 0 \le r' < b \rightarrow ②$

Assume that $q \geq q'$

From ① and ②, $bq + r = bq' + r'$

$\Rightarrow b(q - q') = r' - r \rightarrow ③$ $[\because q \geq q', q - q' \geq 0]$

Hence, $r' - r \geq 0$

But $r' < b$ and $r < b$

$\Rightarrow r' - r < b. \geq 0 \rightarrow ④$

Assume that $q > q'$

Then $q - q' \geq 1$

$\Rightarrow b(q - q') \geq b$ since $b > 0$.

ie, $r' - r \geq b$

This is a contradiction, because $r' - r < b$.

$\therefore q \ngtr q'$ Hence $q = q'$ and Hence $r = r'$

$\therefore$ The integers q and r are unique.

ie. There exist unique integers q and r such that, $a = bq + r, \ 0 \le r < b$.

Scanned with CamScanner

1. Find the quotient and the remainder when the first integer is divided by the second integer:

1) 57, 75 2) −23, 25

$25\,)\,-23\,(-1$
-25
2

H.W. 1) 78, 11 2) 207, 15 3) −23, 5.

$78 = 7(11)+1$ $207 = 13(15)+12$ $-23 = -5(5)+2$

Solution: $q=7, r=1$ $q=13, r=12$ $q=-5, r=2$

$11\,)\,78\,(7$
77
1

1) $57 = 0\times75+57$, where $0 \le 57 < 75$

$\Rightarrow q = 0$ and $r = 57$.

$5\,)\,-23\,(-5$
-25
2

$75\,)\,57\,(0$
0
57

2) $-23 = (-1)(25)+2$, where $0 \le 2 < 25$

$\Rightarrow q = -1,\ r = 2$.

$57 = 0(75)+57$

2. Let $f(n)$ denote the number of positive factors of a positive integer n. Evaluate (i) $f(17)$, (ii) $f(16)$, (iii) $f(12)$.

Solution:

i) The positive factors of 17 are, 1, 17.

$\therefore f(17) = 2$.

ii) The positive factors of 16 are 1, 2, 4, 8, 16.

$\therefore f(16) = 5$

iii) The positive factors of 12 are 1, 2, 3, 4, 6, 12

$\therefore f(12) = 6$.

Theorem: 2 (The pigeonhole principle).

If m pigeons are assigned to n pigeonholes, where $m > n$, then atleast two pigeons must occupy the same pigeonhole.

Proof: Assume the contrary that at most one pigeon occupies each pigeonhole. Then $m \leq n$, a contradiction, Hence the theorem.

Divisibility Relation:

In division algorithm if $r = 0$, then

$$a = bq + r$$

$$\Rightarrow a = bq$$

Then we say that, 'b' divides 'a'

(or) 'b' is a factor of 'a'

(or) 'a' is divisible by 'b'.

(or) 'a' is a multiple of b, and we write $b | a$

If b is not a factor of a, we write $b \nmid a$.

Ex: $3 | 12$, $5 | 30$ but $6 \nmid 5$.

Theorem: 3

Let a and b be positive integers such that $a | b$ and $b | a$ Then $a = b$.

proof: Given: $a|b \Rightarrow b = x\,a \rightarrow ①$

$b|a \Rightarrow a = y\,b \rightarrow ②$

$① \Rightarrow \frac{b}{a} = x$, $② \Rightarrow \frac{a}{b} = y \Rightarrow \frac{b}{a} = \frac{1}{y}$

where $x, y > 0$.

$x = \frac{1}{y}$

$\Rightarrow xy = 1$

$\Rightarrow x = 1, y = 1$

$\therefore a = b$.

Theorem: 4

If $a|b$ and $c|d$ then $ac|bd$.

proof: Given: $a|b \Rightarrow b = x\,a \rightarrow ①$

$c|d \Rightarrow d = y\,c \rightarrow ②$.

$bd = (xy)(ac)$ [$\because$ since $x, y > 0$].

$\Rightarrow ac | bd$.

Theorem: 5

Let a, b, c, d and β be any integers,

Then 1. If $a|b$ and $b|c$ then $a|c$

2. if $a|b$ and $a|c$ then $a|(\alpha b + \beta c)$

3. If $a|b$ then $a|bc$.

Proof:

1) Given: $a|b \Rightarrow b = x\,a$

$b|c \Rightarrow c = y\,b$

Then $c = y\,b = y\,(xa) = xy\,a$

$\Rightarrow c = (xy)\,a$

$\therefore\ a|c.$

2) Given: $a|b \Rightarrow b = x\,a$

$\Rightarrow \alpha b = (\alpha x)\,a$

$a|c \Rightarrow c = y\,a$

$\Rightarrow \beta c = (\beta y)\,a$

Hence, $\alpha b + \beta c = (\alpha x + \beta y)\,a$

$\therefore\ a \,|\, (\alpha b + \beta c).$

3) Given: $a|b \Rightarrow b = x\,a$

$\Rightarrow bc = (cx)\,a$

$= (xc)(a)$

$\Rightarrow a|bc.$

($bc = x\,(ca)$
$\cancel{a}|bc$
$a|b$)

Floor function (or) Greatest integer function:

The floor function of x, denoted by $\lfloor x \rfloor$, is defined as the greatest integer smaller than (or) equal to x.

Ex: $\lfloor 2.1 \rfloor = 2$, $\lfloor 1.99 \rfloor = 1$. $\lfloor -2.33 \rfloor = -3$ and

$\lfloor 3 \rfloor = 3.$

Theorem: 6

Let a and b be any two positive integers. Then the number of positive integers $\leq a$ and divisible by b is $\lfloor a/b \rfloor$.

$S = \{1, \underset{b=2}{2}, 3, \ldots, \underset{a=10}{10}\}$

Proof: Let k be positive integers $\leq a$ and divisible by b.

$\frac{10}{2} = 5^k$

$= \{2, 4, 6, 8, 10\}$

Then these k positive integers are $b, 2b, 3b, \ldots, kb$

$\therefore kb \leq a$ and $(k+1)b > a$.

$k+1 > a/b$

$k > a/b - 1$

$\Rightarrow k \leq \frac{a}{b}$ and $k > \frac{a}{b} - 1 \Rightarrow \frac{a}{b} - 1 < k \leq a/b$

$\Rightarrow k$ is the greatest integer $\leq a/b$

$\Rightarrow k = \lfloor a/b \rfloor$.

Union, intersection and complement:

Let A and B be any two sets.

1) $A \cup B = \{x : x \in A \text{ or } x \in B\}$
2) $A \cap B = \{x : x \in A \text{ and } x \in B\}$
3) $A' = \{x : x \notin A\}$
4) $|A \cup B| = |A| + |B| - |A \cap B|$
5) $|A \cup B \cup C| = |(A \cup B) \cup C|$

$= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$

Inclusion - Exclusion Principle:

Let $A_1, A_2, \ldots, A_n$ be n finite sets.

Then $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j|$

$+ \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1}\left|\bigcap_{i=1}^{n} A_i\right|.$

Even and odd Integers:

In division algorithm if $b=2$ then

$a = 2q+r$ where $0 \le r < 2$.

If $r=0$, then $a=2q$ such Integers 'a' are called even Integers.

If $r=1$, then $a=2q+1$. such integers 'a' are called odd Integers.

1. Find the number of positive integers ≤ 1025 and divisible by 17.

Solution:

A = set of all positive integers ≤ 1025 and divisible by 17.

$= \left\lfloor \frac{1025}{17} \right\rfloor$

$= \left\lfloor 60 \frac{5}{17} \right\rfloor$

$= \lfloor 60.29 \rfloor$

$A = 60.$

Scanned with CamScanner

2. Find the number of positive integers ≤ 3000 and divisible by 3, 5 or 7.

Solution:

Let $A = \{x \in N \,/\, x \le 3000 \text{ and divisible by } 3\}$

$B = \{x \in N \,/\, x \le 3000 \text{ and divisible by } 5\}$

$C = \{x \in N \,/\, x \le 3000 \text{ and divisible by } 7\}$.

By the inclusion - exclusion principle,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

$$= \left\lfloor \frac{3000}{3} \right\rfloor + \left\lfloor \frac{3000}{5} \right\rfloor + \left\lfloor \frac{3000}{7} \right\rfloor - \left\lfloor \frac{3000}{15} \right\rfloor - \left\lfloor \frac{3000}{35} \right\rfloor - \left\lfloor \frac{3000}{21} \right\rfloor + \left\lfloor \frac{3000}{105} \right\rfloor$$

$$= 1000 + 600 + 428 - 200 - 85 - 142 + 28$$

$$\therefore |A \cup B \cup C| = 1629.$$

3. Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

Solution:

Let $A = \{x \in N \,/\, x \le 2076 \text{ and divisible by } 4\}$

$B = \{x \in N \,/\, x \le 2076 \text{ and divisible by } 5\}$

By the inclusion - exclusion principle,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$= \left\lfloor \frac{2076}{4} \right\rfloor + \left\lfloor \frac{2076}{5} \right\rfloor - \left\lfloor \frac{2076}{20} \right\rfloor$$

$$= 519 + 415 - 103 = 831.$$

$|A \cup B| = 831$. $\therefore$ The number of positive integers ≤ 2076 and not divisible by 4 or 5 is, $2076 - 831 = 1245$.

4. Find the number of positive integers ≤ 3076 and
i) divisible by 19   ii) non divisible by 24.

Solution:

1) Let $A = \{x \in N \,/\, x \leq 3076$ and divisible by $19\}$

$$= \left\lfloor \frac{3076}{19} \right\rfloor = \lfloor 161.89 \rfloor$$

$$A = 161.$$

2) $A = \{x \in N \,/\, x \leq 3076$ and not divisible by $24\}$

$$= 3076 - \left\lfloor \frac{3076}{24} \right\rfloor$$

$$= 3076 - 128$$

$$= 2948.$$

5. Find the number of positive integers in the range 1976 through 3776 that are (i) divisible by 13.
(ii) not divisible by 19.

Solution:

(i) The number of positive integers in the range $(1976, 3776]$ that are divisible by 13

$$= \left\lfloor \frac{3776}{13} \right\rfloor - \left\lfloor \frac{1976}{13} \right\rfloor$$

$$= \left\lfloor 290 \tfrac{6}{13} \right\rfloor - \lfloor 152 \rfloor$$

$$= 290 - 152$$

$$= 138.$$

Scanned with CamScanner

ii) The number of positive integers in the range $(1976, 3776]$ that are divisible by 19 is,

$$= \left\lfloor \frac{3776}{19} \right\rfloor - \left\lfloor \frac{1976}{19} \right\rfloor = \left\lfloor 197 \tfrac{14}{19} \right\rfloor - \lfloor 104 \rfloor$$

$$= 197 - 104$$

$$= 93$$

$\therefore$ The number of positive integers in the range that are not divisible by 19 is,

$$= (3776 - 1976) - 93$$

$$= 1800 - 93$$

$$= 1707.$$

Leap year:

A year is a leap year if it is a century divisible by 400 (or) If it is a non-century and divisible by 4.

EX: 2400 and 2016 are leap years and 1900 and 2019 are non-leap years.

6. Show that the number leap years l after 1600 and not exceeding a given year y is given by.

$$l - \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor - 388.$$

Solution:

The given range is $(1600, y]$

Number of leap years in the given range is

$= \{$Number of non-centuries in the range that are divisible by 4$\} + \{$Number of centuries in the range that are divisible by 400$\}$

$= \{$Number of years in the range that are divisible by 4 $-$ Number of centuries in the range$\}$ $+$ $\{$Number of centuries in the range that are divisible by 400$\}$

$$= \left\{\left[\left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{1600}{4} \right\rfloor\right] - \left[\left\lfloor \frac{y}{100} \right\rfloor - \left\lfloor \frac{1600}{100} \right\rfloor\right]\right\} + \left\{\left\lfloor \frac{y}{400} \right\rfloor - \left\lfloor \frac{1600}{400} \right\rfloor\right\}$$

$$\ell = \left\lfloor \frac{y}{4} \right\rfloor - 400 - \left\lfloor \frac{y}{100} \right\rfloor + 16 + \left\lfloor \frac{y}{400} \right\rfloor - 4$$

$$\ell = \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{100} \right\rfloor - 388$$

7. Evaluate each, where d is a positive integer

(i) $\sum_{d|18} d$ (ii) $\sum_{d|12} 1$ (iii) $\sum_{d|18} \frac{1}{d}$ (iv) $\sum_{d|18} \left(\frac{18}{d}\right)$.

Solution:

(i) $\sum_{d|18} d = 1 + 2 + 3 + 6 + 9 + 18$

$= 39$ [$\because$ 1, 2, 3, 6, 9, 18 divide 18]

Scanned with CamScanner

(ii) $\sum_{d|12} 1 = 1+1+1+1+1+1$ [since, 1, 2, 3, 4, 6, 12 are factors of 12]

$= 6.$

(iii) $\sum_{d|18} \left(\frac{1}{d}\right) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} + \frac{1}{9} + \frac{1}{18}$

$= \frac{1}{18}(18+9+6+3+2+1) = \frac{1}{18}(39)$

$= \frac{13}{6}$

(iv) $\sum_{d|18} \left(\frac{18}{d}\right) = \frac{18}{1} + \frac{18}{2} + \frac{18}{3} + \frac{18}{6} + \frac{18}{9} + \frac{18}{18}$

$= 18+9+6+3+2+1$

$= 39.$

8. prove each by cases, when n is an arbitrary integer:

(i) n^2+n is an even integer.

(ii) $2n^3+3n^2+n$ is an even integer.

(iii) n^3-n is divisible by 2.

(iv) $30 | (n^5-n)$.

Solution:

i) $n^2+n = n(n+1)$.

Case (i): Let n be odd

Then $(n+1)$ is even.

∴ The product of an odd integer and an even integer

⇒ an even integer.

⇒ $n(n+1)$ is even.

Case (ii) If n is even, then $(n+1)$ is odd and hence $n(n+1)$ is even.

$2n^2+3n+1$

$2n^2+2n+n+1$

$2n(n+1)+1(n+1)$

(ii) $2n^3+3n^2+n = n(2n^2+3n+1) = n(2n+1)(n+1)$.

$2n+1$ is odd and $n(n+1)$ is even.

$\therefore$ $n(n+1)(2n+1)$ even.

(iii) $n^3-n = n(n^2-1) = n(n-1)(n+1) = (n-1)n(n+1)$

$n-1, n, n+1$ are respectively odd, even, odd (or) even, odd and even.

In either case $(n-1)n(n+1)$ is even.

ie, $(n-1)n(n+1)$ is divisible by 2.

(iv) $30 \mid (n^5-n)$.

Let $n^5-n = n(n^4-1)$

$= n(n^2-1)(n^2+1)$ $(n^2+5n-5n+6-6)$ $n^2-3n+3n+6$

$= n(n-1)(n+1)(n^2-5n+6+5n-5)$

$= n(n-1)(n+1)\left[(n-2)(n-3)+5(n-1)\right]$

$= (n-3)(n-2)(n-1)n(n+1)+5(n-1)^2 n(n+1)$

The first term on the RHS is the product of five consecutive integers.

So it is divisible by $5! = 120$.

Since $3! \mid (n-1)n(n+1)$, the second term on the RHS is divisible by $5 \cdot 6 = 30$.

Hence, the RHS is divisible by $\min\{120, 30\} = 30$.

Scanned with CamScanner

9. prove that the difference of the squares of 2 positive integers cannot be 1.

Solution:

Let x and y be two positive integers.

Then $x+y$ and $x-y$ are 2 distinct integers.

$\therefore \quad (x+y)(x-y) \neq 1$

$\Rightarrow x^2 - y^2 \neq 1.$

10. prove that the product of any 4 consecutive positive integers cannot be a perfect square.

Solution:

Let $n, n+1, n+2, n+3$ be 4 consecutive integers

Then To prove that $n(n+1)(n+2)(n+3)$ cannot be a perfect square.

To prove this assume the contrary that

$n(n+1)(n+2)(n+3) = x^2$, a perfect square.

Then. $n(n+3)(n+1)(n+2) = x^2$

$\Rightarrow (n^2+3n)(n^2+3n+2) = x^2$

$\Rightarrow (n^2+3n)(n^2+3n) + 2(n^2+3n) = x^2$

$\Rightarrow (n^2+3n)^2 + 2(n^2+3n) = x^2$

$\Rightarrow (n^2+3n)^2 + 2(n^2+3n) + 1 = x^2 + 1$

$\Rightarrow (n^2+3n+1)^2 - x^2 = 1$

which is contradiction.

Hence, the product of 4 consecutive positive integers cannot be a perfect square.

11. Show that $2n^3 + 3n^2 + n$ is divisible by 6, By using induction principle, where n is a non-negative integer

Solution:

Let $p(n) = 2n^3 + 3n^2 + n$ is divisible by 6.

$p(0) = 2(0)^3 + 3(0)^2 + 0$

$= 0$ is divisible by 6.

$\therefore$ $p(0)$ is true

Assume that $p(k)$ is true.

ie, $2k^3 + 3k^2 + k$ is divisible by 6.

ie, $2k^3 + 3k^2 + k = 6m$, where m is an integer

now:

$2(k+1)^3 + 3(k+1)^2 + k + 1$

$= 2(k^3 + 3k^2 + 3k + 1) + 3(k^2 + 2k + 1) + k + 1$

$= (2k^3 + 3k^2 + k) + 6k^2 + 12k + 6$

$= 6m + 6(k^2 + 2k + 1)$

$= 6[m + (k+1)^2]$, is divisible by 6.

$\Rightarrow$ $p(k+1)$ is true. whenever $p(k)$ is true

$p(0)$ is true.

$\therefore$ By induction principle $p(n)$ is true for each non-negative integer n.

12. Show that $2^{4n} + 3n - 1$ is divisible by 9, By using induction principle, where n is a non-negative integer.

Solution:

$(a+b)^n = a^n + nC_1 a^{n-1} b + nC_2 a^{n-2} b^2 + \dots + b^n$

Given: $2^{4n} + 3n - 1 = 16^n + 3n - 1$

$= (9+7)^n + 3n - 1$

$= 9^n + nC_1 9^{n-1}(7) + \dots + 7^n + 3n - 1$

$= 9^n + \binom{n}{1} 9^{n-1}(7) + \dots + \binom{n}{n-1} 9(7)^{n-1} + 7^n + 3n - 1$

$= \{\text{integer divisible by } 9\} + 7^n + 3n - 1$

Hence it is enough to prove that $7^n + 3n - 1$ is divisible by 9.

Let $P(n) = 7^n + 3n - 1$ is divisible by 9

Then $P(0) = 7^0 + 3(0) - 1$

$= 1 + 0 - 1$

$P(0) = 0$ is divisible by 9.

$\therefore$ $P(0)$ is true.

Assume that $P(k)$ is true.

i.e. $7^k + 3k - 1$ is divisible by 9.

i.e. $7^k + 3k - 1 = 9m$, where m is an integer.

Now, $7^{k+1} + 3(k+1) - 1 = 7 \cdot 7^k + 3k + 3 - 1$

$= 7(9m - 3k + 1) + 3k + 2$

$= 63m - 21k + 7 + 3k + 2$

$= 63m - 18k + 9$

$= 9(7m - 2k + 1)$ is divisible by 9.

Thus $P(k+1)$ is true whenever $P(k)$ is true. $P(0)$ is true

$\therefore$ By induction principle $P(n)$ is true for all non-negative integers.

Base - b Representation:

The expression $a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$ is the base - b expansion of the integer N.
In this case, we write $N = (a_k a_{k-1} \dots a_1 a_0)_b$ in base b.
When the base is 2, the expansion is called the binary expansion, when b=2, each coefficient is 0 or 1.
Base 8 and base 16 representations are known as octal and hexadecimal representations.
Generally, base 10 to represent any real number, if the base is greater than 10, we use the letters A, B, C, ... to represent the digits 10, 11, 12, ... respectively

1. Express 10110_2 in base 10.

Solution:

$$10110_2 = 1(2^4) + 0(2)^3 + 1(2)^2 + 1(2)^1 + 0(2^0)$$ ← binary expansion.

$$= 16 + 0 + 4 + 2 + 0$$

$$10110_2 = 22$$

2. Express $3ABC_{16}$ in base 10.

Solution:

Here A=10, B=11, C=12;

$$3ABC_{16} = 3(16^3) + 10(16^2) + 11(16^1) + 12(16^0)$$

$$= 12,288 + 2560 + 176 + 12$$

$$= 15,036.$$

3. Express 3014 in base 8.

$8 \overline{)3014}$ — 3008 — 6, quotient 376; $8 \overline{)376}$ — 376 — 0, quotient 47; $8 \overline{)47}$ — 40 — 7, quotient 5; $8 \overline{)5}$ — 0 — 5, quotient 0

Solution:

Given:
$$
\begin{aligned}
3014 &= 376\,(8) + 6 \\
376 &= 47\,(8) + 0 \\
47 &= 5\,(8) + 7 \\
5 &= 0\,(8) + 5
\end{aligned}
$$

$$3014 = 5(8^3) + 7(8^2) + 0(8^1) + 6(8^0)$$
$$= (5706)_8$$

4. Represent 15,036 in the hexadecimal system.

Solution:

Since hexadecimal system is base sixteen.

Given:
$$
\begin{aligned}
15036 &= 939\,(16) + 12 \\
939 &= 58\,(16) + 11 \\
58 &= 3\,(16) + 10 \\
3 &= 0\,(16) + 3
\end{aligned}
$$

$$15036 = 3(16^3) + 10(16^2) + 11(16^1) + 12(16^0)$$
$$= (3ABC)_{16}.$$

HW:

5. Express 1076 in base 2. Ans: $(10000110100)_2$

6. Express 676 in base 8. Ans: $(1244)_8$

Base conversion from Binary to octal:

Group the bits in threes from right to left.

1. Express $(1101)_2$ into octal integer.

Solution:

Given: 1101 = 001, 101

$001 = 0(2^2) + 0(2^1) + 1(2^0) = 1$

$101 = 1(2^2) + 0(2^1) + 1(2^0) = 5$

$\therefore (1101)_2 = (15)_8$

2. Express $(10110101)_2$ into octal integer.

Ans: $(265)_8$

Base conversion from binary to hexadecimal:

Group the bits in fours from right to left.

1. Express $(11101)_2$ in to a hexadecimal digit.

Solution:

Given: 11101 = 0001, 1101

$0001 = 0(2^3) + 0(2^2) + 0(2^1) + 1(2^0) = 1 = 1$

$1101 = 1(2^3) + 1(2^2) + 0(2^1) + 1(2^0) = 13 = D$

$\therefore (11101)_2 = (1D)_{16}$

2. Express $(1110101)_2$ as a hexadecimal digit.

Octal and hexadecimal to Binary:

1. Rewrite 237_{16} as a binary digit.

Solution:

$$2 = 0(2^3)+0(2^2)+1(2^1)+0(2^0) = 0010$$
$$3 = 0(2^3)+0(2^2)+1(2^1)+1(2^0) = 0011$$
$$7 = 0(2^3)+1(2^2)+1(2^1)+1(2^0) = 0111$$

$$(237)_{16} = (001000110111)_2$$
$$= (1000110111)_2$$

2 | 2
1 – 0

2 | 3
1 – 1

2 | 7
2 | 3 – 1
1 – 1

2. Express $3AD_{16}$ as a binary digit.

Solution:

$$3 = 0(2^3)+0(2^2)+1(2^1)+1(2^0) = 0011 = 0011$$
$$A = 10 = 1(2^3)+0(2^2)+1(2^1)+0(2^0) = 1010$$
$$D = 13 = 1(2^3)+1(2^2)+0(2^1)+1(2^0) = 1101$$

$$(3AD)_{16} = (001110101101)_2$$
$$= (1110101101)_2$$

2 | 3
1 – 0

2 | 10
2 | 5 – 0
2 | 2 – 1
1 – 0

2 | 13
2 | 6 – 1
2 | 3 – 0
1 – 1

3. Rewrite $(237)_8$ as a binary digit.

3. Number patterns:

1. Study the following number pattern write down the n^{th} row and prove that validity of the number pattern.

$$1 \times 9 + 2 = 11$$
$$12 \times 9 + 3 = 111$$
$$123 \times 9 + 4 = 1111$$
$$1234 \times 9 + 5 = 11111 \quad \text{etc.,}$$

Solution:

To prove that $123\ldots(n) \times 9 + (n+1) = \underbrace{111\ldots11}_{n+1 \text{ ones}} \rightarrow (1)$

(1) →

$$\text{L.H.S} = (123\ldots n) \times 9 + (n+1)$$
$$= 9\left[1.10^{n-1} + 2.10^{n-2} + 3.10^{n-3} + \ldots + n.10^0\right] + (n+1)$$
$$= (10-1)\left[1.10^{n-1} + 2.10^{n-2} + 3\ 10^{n-3} + \ldots + n.10^0\right] + (n+1)$$
$$= 1.10^n + 2.10^{n-1} + 3.10^{n-2} + \ldots + n.10^1$$
$$- \left(1.10^{n-1} + 2.10^{n-2} + \ldots + (n-1).10^1 + n.10^0\right) + (n+1).$$
$$= 10^n + 10^{n-1} + 10^{n-2} + \ldots + 10^1 - n + n + 1$$
$$= \underbrace{111\ldots11}_{(n+1) \text{ ones}}$$

2. Add two more rows to the following pattern, Conjecture a formula for the n^{th} row and prove it.

$$9 \times 9 + 7 = 88$$
$$98 \times 9 + 6 = 888$$
$$987 \times 9 + 5 = 8888$$
$$9876 \times 9 + 4 = 88888$$
$$98765 \times 9 + 3 = 888888 \quad \text{etc.}$$

Solution:

The next two rows of the pattern are

$$987654 \times 9 + 2 = 8888888$$

$$9876543 \times 9 + 1 = 88888888$$

The n^{th} row is given by,

$$987\ldots(10-n) \times 9 + (8-n) = \underbrace{888\ldots88}_{(n+1)\text{ eights.}} \longrightarrow ①$$

$$\text{LHS of } ① = \underbrace{987\ldots(10-n)}_{n \text{ terms}} \times 9 + (8-n)$$

$$= 9\left[9 \times 10^{n-1} + 8 \times 10^{n-2} + 7 \times 10^{n-3} + \ldots + (10-(n-1)) \times 10^{1} + (10-n) \times 10^{0}\right] + 8 - n$$

$$= (10-1)\left[9 \times 10^{n-1} + 8 \times 10^{n-2} + 7 \times 10^{n-3} + \ldots + (10-(n-1)) \times 10^{1} + (10-n)\right] + 8 - n$$

$$= 9 \times 10^{n} + 8 \times 10^{n-1} + 7 \times 10^{n-2} + \ldots + (11-n)10^{2} + (10-n) \times 10 - \left[9 \times 10^{n-1} + 8 \times 10^{n-2} + \ldots + (12-n) \times 10^{2} + (11-n) \times 10 + (10-n)\right] + 8 - n$$

$$= 9 \times 10^{n} - 10^{n-1} - 10^{n-2} + \ldots - 10^{2} - 10 - (10-\cancel{n}) + 8 - \cancel{n}$$

$$= 9 \times 10^{n} - \left[10 + 10^{2} + \ldots + 10^{n-1}\right] - 2$$

$$= 9 \times 10^{n} - 10\frac{(10^{n-1} - 1)}{(10-1)} - 2$$

$$= 9 \times 10^{n} - \frac{10}{9} \times 10^{n-1} + \frac{10}{9} - 2$$

$$= \frac{81 \times 10^{n} - 10^{n}}{9} + \left(\frac{10-18}{9}\right) = \frac{80 \times 10^{n}}{9} - \frac{8}{9} = \frac{8}{9} \times 10^{n+1} - \frac{8}{9}$$

$$= \frac{8}{9}(10^{n+1} - 1)$$

$$= \frac{8}{9}\left[\underbrace{999\ldots9}_{(n+1)\text{ times}}\right] = \underbrace{888\ldots88}_{(n+1)\text{ times}} = \text{RHS.}$$

4. Prime and Composite Numbers:

A positive integer $p > 1$ is called a prime number if its only positive factors are 1 and p.

A positive integer greater than 1 is called a composite number if it is not a prime.

By the definition 1 is neither a prime nor a composite.

Theorem: 1

Every integer $n \geq 2$ has a prime factor.

Proof:

We prove this theorem using, strong induction.

Integer 2 has a prime factor 2.

Assume that all integers n such that $2 \leq n \leq k$ have a prime factor.

Now, we prove that $k+1$ has a prime factor.

Case (i) Let $k+1$ be a prime

Then $k+1$ has a prime factor $k+1$.

Case (ii) Let $k+1$ be not a prime.

Then $k+1$ is a composite number.

$\therefore$ $k+1$ has a factor $d \leq k$ and $d \geq 2$.

Hence by assumption, d has a prime factor and

$\therefore$ $k+1$ has a prime factor.

Thus by the principle of strong induction every integer $n \geq 2$ has a prime factor.

Theorem: 2. (Euclid)

There are infinitely many primes.

Proof: Assume the contrary that there are only finite number of primes $p_1, p_2, \ldots, p_n$.

consider the integer,

$$N = p_1 p_2 \ldots p_n + 1$$

If $N \geq 2$, $\therefore$ N has a prime factor, say p_i, $1 \leq i \leq n$, by the above theorem,

Hence $p_i \mid N$ and $p_i \mid p_1 p_2 \ldots p_n$.

$$\Rightarrow p_i \mid (N - p_1 p_2 \ldots p_n)$$

$$\Rightarrow p_i \mid 1, \text{ with } p_i \text{ prime.}$$

This is a contradiction.

$\therefore$ There are infinitely many primes.

Primes and π function:

Let x be a positive real number.

Then $\pi(x)$ denotes the number of primes $\leq x$.

Ex: $\pi(10) = 4$, $\pi(100) = 25$

In general,

$$\pi(x) = \sum_{p \leq x} 1, \text{ where } p \text{ denotes a prime.}$$

Theorem: 3

Let $p_1, p_2, \ldots, p_t$ be primes $\leq \sqrt{n}$.

Proof: Let $\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_{i} \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor$

$$- \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \cdots + (-1)^t \left\lfloor \frac{n}{p_1 p_2 \cdots p_t} \right\rfloor.$$

Theorem: 4 [Prime Number theorem]

As x gets larger and larger $\pi(x)$ approaches to $\frac{x}{\ln x}$, $x \geq 2$. i.e., $\lim_{x \to \infty} \frac{\pi(x)}{(x/\ln x)} = 1$, $x \geq 2$.

Theorem: 5

For every positive integer n, there are n consecutive integers that are composite numbers.

Proof: Consider the n consecutive integers $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$.

where $n \geq 1$. Let $2 \leq k \leq n+1$. Then

$k \mid (n+1)!$ and $k \mid k$

$\Rightarrow$ $k \mid [(n+1)! + k]$, for every $k = 2, 3, \ldots, (n+1)$.

$\Rightarrow$ $2 \mid [(n+1)!+2]$, $3 \mid [(n+1)!+3]$, $\ldots$, $(n+1) \mid [(n+1)!+(n+1)]$

$\Rightarrow$ $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$ are n consecutive integers which are composite numbers.

Theorem: 6

Every composite number n has a prime factor $\leq \lfloor \sqrt{n} \rfloor$, the greatest integer $\leq \sqrt{n}$.

Proof:
Given n is composite
$\Rightarrow$ there are integers a and b such that $n = ab$,
where $1 < a < n$, $1 < b < n$.
Suppose that $a > \sqrt{n}$ and $b > \sqrt{n}$.
Then $n = ab > \sqrt{n}\sqrt{n} = n$, a contradiction.
$\therefore$ Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
Since, both a and b are integers either $a \leq \lfloor \sqrt{n} \rfloor$ (or) $b \leq \lfloor \sqrt{n} \rfloor$.
By theorem: (1) every integer ≥ 2 has a prime factor.
$\therefore$ "a" has a prime factor p.
Hence p is a prime factor of $ab (= n)$ and $p \leq a \leq \lfloor n \rfloor$
Thus n has a prime factor $\leq \lfloor \sqrt{n} \rfloor$.

Note:
"If n has no prime factor $\leq \lfloor \sqrt{n} \rfloor$, then n is a prime."

1. Determine whether 1601 is a prime number.

Solution: Primes $\leq \lfloor \sqrt{1601} \rfloor$ are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 and 37.
Note that none of 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 and 37 divides $n = 1601$. ie., $n = 1601$ has no prime factor $\leq \sqrt{n} = \lfloor \sqrt{1601} \rfloor$, $\therefore$ by the above note $n = 1601$ is a prime.

Scanned by CamScanner

Theorem: 7.

Prove that there is no polynomial with integral coefficients that will produce primes for all integers n.

Proof: Assume the contrary that there is a polynomial with integral coefficients

Let $f(n) = a_k n^k + a_{k-1} n^{k-1} + \dots + a_1 n + a_0$

where $a_k \neq 0$.

Let b be some integer.

Since $f(n)$ is always a prime, $f(b)$ must be a prime.

ie., $f(b) = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0 = p \rightarrow ①$.

Let t be an arbitrary integer.

Then $f(b+tp) = a_k (b+tp)^k + a_{k-1} (b+tp)^{k-1} + \dots + a_1 (b+tp) + a_0$.

$$= (a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0) + p \cdot g(t).$$

$$= p + p\,g(t), \text{ (by ①)}$$

$$= p(1 + g(t))$$

$\Rightarrow p \mid f(b+tp)$ with $f(b+tp)$ prime.

$\Rightarrow p = f(b+tp)$.

$\Rightarrow f$ takes on the same value infinitely many times, since t is arbitrary.

But $f(n)$ is a polynomial of degree k and so it cannot assume the same value more than k times.

This contradiction proves the desired result.

Theorem: 8

For every positive integer n, there are n consecutive integers that are composite numbers.

Proof: consider the n consecutive integers,

$(n+1)!+2,\ (n+1)!+3, \ldots, (n+1)!+(n+1)$,

where $n \geq 1$. Let $2 \leq k \leq n+1$.

Then $k \mid (n+1)!$ and always $k \mid k$.

$\Rightarrow k \mid [(n+1)!+k]$, for every $k = 2, 3, \ldots, (n+1)$.

$\Rightarrow 2 \mid [(n+1)!+2],\ 3 \mid [(n+1)!+3], \ldots, (n+1) \mid [(n+1)!+(n+1)]$

$\Rightarrow (n+1)!+2,\ (n+1)!+3, \ldots, (n+1)!+(n+1)$ are n consecutive integers which are composite numbers.

1. Using the above result, find the number of primes ≤ 100

Solution:

Let $n = 100$ and $\sqrt{n} = \sqrt{100} = 10$.

primes which are less than or equal to 10 are:

2, 3, 5, 7.

$$\pi(100) = 100 - 1 + \pi(\sqrt{100}) - \left\{ \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor \left\lfloor \frac{100}{7} \right\rfloor \right\}$$

$$+ \left\{ \left\lfloor \frac{100}{2\times3} \right\rfloor + \left\lfloor \frac{100}{2\times5} \right\rfloor + \left\lfloor \frac{100}{2\times7} \right\rfloor + \left\lfloor \frac{100}{3\times5} \right\rfloor + \left\lfloor \frac{100}{3\times7} \right\rfloor + \left\lfloor \frac{100}{5\times7} \right\rfloor \right\}$$

$$- \left\{ \left\lfloor \frac{100}{2\times3\times5} \right\rfloor + \left\lfloor \frac{100}{2\times3\times7} \right\rfloor + \left\lfloor \frac{100}{2\times5\times7} \right\rfloor + \left\lfloor \frac{100}{3\times5\times7} \right\rfloor \right\}$$

$$+ \left\lfloor \frac{100}{2\times3\times5\times7} \right\rfloor$$

$= 99 + 4 - \{50 + 33 + 20 + 14\} + \{16 + 10 + 7 + 6 + 4 + 2\}$
$- \{3 + 2 + 1 + 0\} + 0$

$= 103 - 117 + 45 - 6$

$= 148 - 123$

$\pi(100) = 25$

2. Find six consecutive integers that are composites.

Solution:

By the above Theorem 8 consecutive composite numbers are $(6+1)! + 2$, $(6+1)! + 3$, $(6+1)! + 4$, $(6+1)! + 5$, $(6+1)! + 6$, $(6+1)! + 7$.

ie., $7! + 2, 7! + 3, 7! + 4, 7! + 5, 7! + 6, 7! + 7$.

ie., 5042, 5043, 5044, 5046, 5047.

Greatest Common Divisor (GCD):

The gcd of two integers a and b, not both zero, is the largest positive integer that divides both a and b, it is denoted by (a, b).

Ex: $(3, 15) = 3$, $(1, 17) = 1$, $(15, 25) = 5$, $(3, 0) = 3$.
$(12, 18) = 6$, $(11, 13) = 1$, $(4, 0) = 4$.

symbolic definition of gcd:

A positive integer d is the gcd of two positive integers a and b if

(i) $d|a$ and $d|b$

(ii) if $d'|a$ and $d'|b$ then $d' \leq d$. (or) $d'|d$.

where d' is also a positive integer.

Relatively Prime Integers:

Two positive integers a and b are relatively prime if their gcd is 1.

i.e., if $(a, b) = 1$.

Ex: $(6, 35) = 1$.

Properties of gcds:

1. Let $(a,b) = d$ Then.

1. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

2. $(a, a-b) = d$.

L.C

3	12
2	4
2	2
	1

3×2^2

3	18
3	6
2	2
	1

$3^2 \times 2^1$

gcd $\{12, 18\} = 6$

gcd $= 3 \times 2 = 6 = \alpha a + \beta b$

$= 1.18 + (-1)12$

$= 18 - 12 = 6$.

Linear Combination:

A linear combination of the integers a and b is a sum of Multiples of a and b that is, a sum of the form $\alpha a + \beta b$, where α and β are integers.

Theorem: 1 (Euler)

The gcd of the positive integers a and b is a linear combination of a and b.

Proof:

Let $S = \{ ma+nb \mid ma+nb > 0,\ m,n \in \mathbb{Z} \}$

(i) To show that S has a least element:

Since $a = 1 \cdot a + 0 \cdot b$ and $a > 0$, $a \in S$

i.e., $S \neq \phi$, S is non-empty.

So by the well ordering principle, S has a least element d.

(ii) To show that $d = (a,b)$:

Since $d \in S \Rightarrow d = \alpha a + \beta b$, where $\alpha, \beta \in \mathbb{Z}$.

Given integers a and d, by division algorithm, there exist integers q and r such that.

$$a = qd + r \quad \rightarrow (1) \quad \text{where } 0 \leq r < d.$$

$$(1) \Rightarrow r = a - qd$$

$$= a - q(\alpha a + \beta b)$$

$$= a - q\alpha a - a\beta b$$

$$r = (1 - q\alpha)a + (-q\beta)b$$

$\Rightarrow$ This show that r is a linear combination of a and b.

If $r > 0$ then $r \in S$, since $r < d$, r is less than the smallest element in S. which is a contradiction.

$\therefore r = 0$, Hence from ①, $a = qd \Rightarrow d|a$.

Ily $d|b$; Thus d is a common factor of a and b.

Now, suppose that $d'|a$ and $d'|b$.

Then $d'|(\alpha a + \beta b)$ ie., $d'|d$ ie, $d' \leq d$.

Hence d is a gcd of a, b.

$\therefore$ $d = (a, b)$ and $d = \alpha a + \beta b$.

Theorem: 2

If $d = (a, b)$ and if d' is a common factor of a, b then $d'|d$.

proof: since $d = (a, b) \Rightarrow d = \alpha a + \beta b$, for some $\alpha, \beta \in \mathbb{Z}$.

d' is a common factor of a and b.

$\Rightarrow d'|a$ and $d'|b$

$\Rightarrow d'|(\alpha a + \beta b) \Rightarrow d'|d$.

Theorem: 3

Let a, b and c be any three positive integers. Then $(ac, bc) = c(a, b)$.

proof: Let $d = (a, b) \Rightarrow d = \alpha a + \beta b$ for some integers α and β.

Then $dc = \alpha(ac) + \beta(bc)$

$\Rightarrow dc = (ac, bc)$

$\Rightarrow c(a,b) = (ac, bc)$.

Theorem: 4

Two positive integers a and b are relatively prime iff there are integers α and β such that $\alpha a + \beta b = 1$.

Proof: Assume that a and b are relatively prime.

Then $(a,b) = 1$.

W.K.T, there exists integers α and β such that

$$(a,b) = \alpha a + \beta b$$

$$\Rightarrow 1 = \alpha a + \beta b.$$

Conversely, assume that there exists integers α and β such that $\alpha a + \beta b = 1$.

Let $d = (a,b)$. Then $d|a$ and $d|b$.

$\Rightarrow d \mid (\alpha a + \beta b) \Rightarrow d|1 \Rightarrow d = 1$ (since d is a positive integer).

$\Rightarrow (a,b) = 1 \Rightarrow a$ and b are relatively prime.

Cordlary: 1

If $d = (a,b)$ then $(a/d, b/d) = 1$.

Proof: Given: d is a gcd $\Rightarrow d$ is a +ve integer

$$d = (a,b) \Rightarrow d = \alpha a + \beta b$$
$$\Rightarrow 1 = \alpha(a/d) + \beta(b/d)$$
$$\Rightarrow (a/d, b/d) = 1.$$

Corollary: 3 If $(a,b) = 1 = (a,c)$ then $(a,bc) = 1$.

Proof:

Given: $(a,b) = 1 \Rightarrow$ there exist integers α and β such that $\alpha a + \beta b = 1. \rightarrow ①$

$(a,c) = 1 \Rightarrow$ there exist integers γ and δ such that $\gamma a + \delta c = 1 \rightarrow ②$

using ② in ① $\Rightarrow \alpha a + \beta b = 1 \Rightarrow \alpha a + \beta b(1) = 1.$

$$\Rightarrow \alpha a + \beta b(\gamma a + \delta c) = 1$$
$$\Rightarrow (\alpha a) + \beta\gamma ba + \beta\delta bc = 1$$
$$\Rightarrow (\alpha + \beta\gamma b)a + (\beta\delta)bc = 1$$

$\Rightarrow$ By the above theorem $(a,bc) = 1$.

Corollary: 4 If $a|c$ and $b|c$ and $(a,b) = 1$ then $ab|c$.

Proof:

Given: $a|c \Rightarrow c = am \rightarrow ①$

$b|c \Rightarrow c = bn \rightarrow ②$

$\Rightarrow (a,b) = 1 \Rightarrow$ there exist integers α and β such that $\alpha a + \beta b = 1. \rightarrow ③$

Scanned by CamScanner

$③ \Rightarrow \alpha ac + \beta bc = c$

$\Rightarrow \alpha a(bn) + \beta b(am) = c$ using ② & ①.

$\Rightarrow (\alpha n + \beta m) ab = c$

$\Rightarrow ab | c.$

Corollary: 5 (Euclid)

If a and b are relatively prime, and if $a|bc$, then $a|c$.

Proof: Given a and b are relatively prime.

$\Rightarrow (a, b) = 1$

$\Rightarrow \alpha a + \beta b = 1$; $\exists\ \alpha, \beta \in \mathbb{Z}$.

$\Rightarrow \alpha\ ac + \beta\ bc = c \quad \rightarrow ①$

Since $a | \alpha ac$ and $a | \beta bc \Rightarrow a | \alpha ac + \beta bc$

$\Rightarrow a|c$ by ①.

1. Using recursion, evaluate $(18, 30, 60, 75, 132)$.

Solution:

Given: $(18, 30, 60, 75, 132) = ((18, 30, 60, 75), 132)$

$= (((18, 30, 60), 75), 132)$

$= ((((18, 30), 60), 75), 132)$

$= (((6, 60), 75), 132)$

$= ((6, 75), 132)$

$= (3, 132)$

$= 3.$

Ex:

6	18, 30
	3, 5
6	6, 60
	1, 10
3	6, 75
	2, 25
3	3, 132

H.W

2. $(12, 18, 28, 38, 44)$.

Scanned by CamScanner

The Euclidean Algorithm:

Theorem: 1

Let a, b be any two positive integers, and r the remainder, when a is divided by b. Then $(a, b) = (b, r)$.

Proof: Let $d = (a, b)$ and $d' = (b, r)$

By division algorithm, there exists a unique q such that

$a = bq + r$

$$d = (a, b) \Rightarrow d \mid a \text{ and } d \mid b$$
$$\Rightarrow d \mid a \text{ and } d \mid bq$$
$$\Rightarrow d \mid (a - bq)$$
$$\Rightarrow d \mid r$$

$d \mid b$ and $d \mid r \Rightarrow d \mid (b, r) \Rightarrow d \mid d' \Rightarrow d \leq d' \rightarrow (1)$

$$d' = (b, r) \Rightarrow d' \mid b \text{ and } d' \mid r$$
$$\Rightarrow d' \mid bq \text{ and } d' \mid r$$
$$\Rightarrow d' \mid (bq + r)$$
$$\Rightarrow d' \mid a$$

$d' \mid a$ and $d' \mid b \Rightarrow d' \mid (a, b)$

$\Rightarrow d' \mid d \Rightarrow d' \leq d \longrightarrow (2)$

From (1) and (2),

$d = d'$ i.e., $(a, b) = (b, r)$.

1. Evaluate $(2076, 1776)$.

Solution:

$$\overset{a}{2076} = \overset{q}{1} \cdot \overset{b}{1776} + \overset{r}{300}$$

$$1776 = 5 \cdot 300 + 276$$

$$300 = 1 \cdot 276 + 24$$

$$276 = 11 \cdot 24 + 12 \quad \text{(last non-zero remainder)}$$

$$24 = 2 \cdot 12 + 0$$

By the above thm,

$$\because (2076, 1776) = (1776, 300) = (300, 276)$$
$$= (276, 24) = (24, 12)$$
$$= 12.$$

$\therefore$ The last non-zero remainder $= 12$.

2. Apply the Euclidean algorithm to find $(4076, 1024)$.

Solution:

$$4076 = 3 \cdot 1024 + 1004 \quad \rightarrow (1)$$

$$1024 = 1 \cdot 1004 + 20 \quad \rightarrow (2)$$

$$1004 = 50 \cdot 20 + 4 \quad \rightarrow (3)$$

$$20 = 5 \cdot 4 + 0$$

$\Rightarrow$ The last non-zero remainder is $= 4$

$\Rightarrow (4076, 1024) = 4.$

3. Express (4076, 1024) as a linear combination:

Solution:

$$(4076, 1024) = 4$$
$$= 1004 - 50 \cdot 20 \text{ by } ③$$
$$= 1004 - 50(1024 - 1.1004) \text{ by } ②$$
$$= 51.1004 - 50 \cdot 1024$$
$$= 51.(4076 - 3 \cdot 1024) - 50 \cdot 1024$$
$$= 51 \cdot 4076 - 153.1024 - 50.1024$$
$$= 51 \cdot 4076 + (-203)\, 1024$$

A linear combination of 4076 and 1024.

The fundamental Theorem of Arithmetic:

Lemma: (Euclid).

If p is a prime and $p|ab$ then $p|a$ (or) $p|b$.

Proof: Let $p \nmid a$.

Then $(p, a) = 1$.

$\therefore$ There exists integers α and β such that,

$$(p, a) = \alpha p + \beta a = 1$$

$$\Rightarrow \alpha pb + \beta ab = b \longrightarrow ①$$

$p | \alpha pb$ and $p | ab$

$$\Rightarrow p | (\alpha pb + \beta ab)$$

$$\rightarrow p | b \quad (\text{by } ①)$$

Scanned by CamScanner

Fundamental Theorem of Arithmetic:

Statement:

Every integer $n (\geq 2)$ either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof: Let $p(n)$: n is a prime or can be expressed as a product of primes.

Since 2 is a prime, the statement $p(2)$ is true.

Assume that the statement $p(2), P(3), \ldots, p(k)$ are true.

i.e., m is a prime or m can be expressed as a product of primes for $2 \leq m \leq k$.

Now consider the integer $k+1$.

If $k+1$ is prime, then $p(k+1)$ is true.

If $k+1$ is composite, then $k+1 = ab$, where $2 \leq a, b < k+1$.

Hence by assumption: Either

(i) a is prime and b is prime (or)

(ii) a is prime and b can be expressed as a product of primes (or)

(iii) Both a and b can be expressed as product of primes.

In any case, $k+1 =$ a product of primes.

$\therefore$ $p(k+1)$ is true, whenever $p(2), p(3), \ldots p$ are all true.

Hence, by Strong induction, $p(n)$ is true.

Uniqueness part:

Let $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ with $r \le s$.

proof is similar if $r \geq s$.

$p_1 \mid p_1 . p_2 \ldots p_r$ and $p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$

$\Rightarrow p_1 \mid q_1 q_2 \ldots q_s$ with $p_1, q_1, q_2, \ldots, q_s$ are all prime

$\Rightarrow$ By the above corollary, [if $p, q_1, q_2, \ldots, q_n$ are primes such that $p \mid q_1 q_2 \ldots q_n$ then $p = q_i$ for some i]

$\Rightarrow p_1 = q_i$ for some i, $1 \le i \le s$.

$\therefore$ $\cancel{p_1} p_2 \ldots p_r = q_1 q_2 \ldots q_{i-1} \cancel{q_i} q_{i+1} \ldots q_s \to (1)$

Again, by the same corollary, $(1) \Rightarrow p_2 = q_j$ for some j with $1 \le j \le s$ and $j \ne i$.

Since $r \le s$, continuing like this, we can cancel every p_t with some q_k.

This yields a 1 on the lhs at the end. Then the rhs cannot be left with any primes,

Since product of primes can never yield a 1.

$\therefore$ $r = s$ and hence the primes $q_1, q_2, \ldots, q_s$ are the same as the primes $p_1, p_2, \ldots p_r$ in some order.

Hence, the factorization of n is unique, except for the order.

Least Common Multiple (LCM):

The least common multiple of two positive integers a and b is the last positive integer divisible by both a and b ; It is denoted by [a, b].

LCM using canonical Decomposition:

Let a and b be two positive integers with following canonical decompositions:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \; ; \; b = p_1^{b_1} p_2^{b_2}, \ldots p_n^{b_n}$$

where $a_i, b_i \geq 0$.

Then, $[a, b] = p_1^{Max[a_1, b_1]} p_2^{Max[a_2, b_2]} \cdots p_n^{Max[a_n, b_n]}$

Theorem:

Let a and b be positive integers.

Then $[a, b] = \dfrac{ab}{(a, b)}$.

Proof: Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2}, \ldots p_n^{b_n}$

be the canonical decomposition of a and b.

Then $[a, b] = p_1^{Max\{a_1, b_1\}} \cdot p_2^{Max\{a_2, b_2\}} \cdots p_n^{Max\{a_n, b_n\}}$

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

$$\Rightarrow [a, b](a, b) = p_1^{max\{a_1, b_1\} + min\{a_1, b_1\}} \cdots p_n^{min\{a_n, b_n\} + max\{a_n, b_n\}}$$

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

$$= \left(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}\right)\left(p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}\right)$$

$$\Rightarrow [a,b] = \frac{ab}{(a,b)}.$$

1. Using the canonical decompositions of 1050 and 2574.

Solution:

$$1050 = 2 \times 525 = 2 \times 5 \times 105$$

$$= 2 \times 5 \times 5 \times 21$$

$$= 2 \times 5^2 \times 3 \times 7$$

$$= 2^1 \times 3^1 \times 5^2 \times 7^1$$

$$2574 = 2 \times 1287 = 2 \times 3 \times 429$$

$$= 2 \times 3 \times 3 \times 143$$

$$= 2 \times 3^2 \times 11 \times 13$$

$$\Rightarrow 1050 = 2^1 \times 3^1 \times 5^2 \times 7^1 \times 11^0 \times 13^0 \text{ and}$$

$$2574 = 2^1 \times 3^2 \times 5^0 \times 7^0 \times 11^1 \times 13^1$$

$$\Rightarrow [1050, 2574] = 2^{Max\{1,1\}} \cdot 3^{Max\{1,2\}} \cdot 5^{Max\{0,2\}} \, 7^{Max\{0,1\}} \cdot 11^{Max\{0,1\}} \cdot 13^{Max\{0,1\}}$$

$$= 2^1 . 3^2 . 5^2 . 7^1 . 11^1 . 13^1$$

$$= 2 \times 9 \times 25 \times 77 \times 13$$

$$= 450450.$$

2. Using $(252, 360)$ compute $[252, 360]$.

Solution:

$$252 = 2 \times 126 = 2 \times 2 \times 63$$

$$= 2^2 \times 3^2 \times 7^1$$

$$360 = 2 \times 180 = 2 \times 2 \times 90$$

$$= 2^3 \times 3^2 \times 5^1$$

$$\Rightarrow (252, 360) = 2^2 \times 3^2 = 36$$

$$\Rightarrow [252, 360] = \frac{252 \times 360}{(252, 360)} = \frac{252 \times 360}{36}$$

$$[252, 360] = 2520$$

3. If a and b are relatively prime, then $[a, b] = ab$.

Proof: Given: a, b are relatively prime.

$$\Rightarrow (a, b) = 1$$

$$\therefore [a, b] = \frac{ab}{(a, b)} = \frac{ab}{1}$$

$$\therefore [a, b] = ab.$$