UNIT III

DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS

1.State and prove the division algorithm in divisibility theory

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

PROOF

The proof consists of two parts.

First, we must establish the existence of the integers q and r, and then we must show they are indeed unique.

1) EXISTENCE PROOF

Consider the set $S = \{a - bn \mid (n \in Z) \text{ sand } (a - bn \geq 0)\}$.

Clearly, $S \subseteq W$.

We shall show that S contains a least element.

Tofirst we will show that S is a nonempty subset of W:

Case 1 Suppose $a \geq 0$. Then $a = a - b \cdot 0 \in S$, so S contains an element.

Case 2 Suppose $a < 0$. Since $b \in Z+$, $b \geq 1$. Then $-ba \geq -a$;

that is, $a - ba \geq 0$. Consequently, $a - ba \in S$.

In both cases, S contains at least one element,

so S is a nonempty subset of W.

Therefore, by the well-ordering principle, S contains a least element r.

Since $r \in S$, an integer q exists such that $r = a - bq$, where $r \geq 0$.

To show that r < b:

We will prove this by contradiction.

Assume $r \geq b$. Then $r - b \geq 0$.

But $r - b = (a - bq) - b = a - b(q + 1)$.

Since $a - b(q + 1)$ is of the form $a - bn$ and is ≥ 0, $a-b(q+1) \in S$;

that is, $r -b \in S$. Since $b > 0$, $r -b < r$.

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

This contradicts our choice of r, so $r < b$.

Thus, there are integers q and r such **that a = bq + r, where $0 \leq r < b$**.

UNIQUENESS

We would like to show that the integers q and r are unique.

Assume there are integers q, q' , r and r'such that a = bq + r and a = bq' + r' , where $0 \le r < b$ and $0 \le r' < b$.

Assume, for convenience, that $q \ge q'$.

Then $r' - r = b(q - q')$.

Because $q \ge q'$, $q - q' \ge 0$ and hence $r' - r \ge 0$.

But, because $r' < b$ and $r < b$, $r' - r < b$.

Suppose $q > q'$; that is, $q - q' \ge 1$.

Then $b(q - q') \ge b$; that is, $r' - r \ge b$.

This is a contradiction because $r' - r < b$. Therefore, $q \not> q'$; thus, $q = q'$, and hence, $r = r'$.

Thus, the integers q and r are unique, completing the uniqueness proof.

Definition:Pigeonhole principle:

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

2.Let b be an integer ≥ 2. Suppose b+1 integers are randomly selected. Prove that the difference of two of them is divisible by b.

PROOF:

Let q be the quotient and r the remainder when an integer a is divided by b.

Then,by the division algorithm, $a = bq + r$, where $0 \le r < b$.

The b + 1 integers yield b + 1 remainders (pigeons), but there are only b possible remainders (pigeonholes).

Therefore, by the pigeonhole principle, two of the remainders must be equal.

Let x and y be the corresponding integers.

Then $x = bq_1 + r$ and $y = bq_2 + r$ for some quotients q_1 and q_2.

Therefore,

$$x - y = (bq_1 + r) - (bq_2 + r)$$
$$= b(q_1 - q_2)$$

Thus, x-y is divisible by b

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

SOLUTION
Let A = {x ∈ N | x ≤ 2076 and divisible by 4} and B = {x ∈ N | x ≤ 2076 and divisi-ble by 5}.

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

$= 2076/4 + 2076/5 - 2076/20$

$= 519 + 415 - 103$

$= 831$

Thus, among the first 2076 positive integers, there are $2076 - 831 = 1245$ integers not divisible by 4 or 5.

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

SOLUTION
Let A, B, and C denote the sets of positive integers ≤ 3000 and divisible by 3, 5, or 7.
By the inclusion–exclusion principle,

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

$= 3000/3 + 3000/5 + 3000/7 - 3000/15 - 3000/35$

$- 3000/21 + 3000/105$

$= 1000 + 600 + 428 - 200 - 85 - 142 + 28 = 1629$

5.Express 3014 in base eight.
SOLUTION
The largest power of 8 that is contained in 3014 is 512.
Apply the division algorithmwith 3014 as the dividend and 512 as the divisor:

$3014 = 5 \cdot 512 + 454$

Now look at 454. It lies between 64 and 512. The largest power of 8 we can now use is 64:

$454 = 7 \cdot 64 + 6$

Continue like this until the remainder becomes less than 8:

$6 = 6 \cdot 1 + 0$

Thus, we have

$$\begin{aligned} 3014 &= 5(512) + 7(64) + 6 \\ &= 5(8^3) + 7(8^2) + 0(8^1) + 6(8^0) \\ &= 5706_{\text{eight}} \end{aligned}$$

6.Every integer n ≥ 2 has a prime factor.

PROOF (by strong induction)

The given statement is clearly true when n = 2.

Now assume it is true for every positive integer $n \leq k$, where $k \geq 2$.

Consider the integer k + 1.

case 1 If k + 1 is a prime, then k + 1 is a prime factor of itself.

case 2 If k + 1 is not a prime, k + 1 must be a composite,

so it must have a factor $d \leq k$.

Then, by the inductive hypothesis, d has a prime factor p.

So p is a factor ofk + 1,

Thus, by the strong version of induction, the statement is true for every integer

≥ 2;

that is, every integer ≥ 2 has a prime factor.

7.Prove that there are infinitely many primes.

PROOF (by contradiction)

Assume there is only a finite number of primes, p1, p2,..., pn. Consider the integer

$N = p1p2 \cdots pn + 1$. Since $N \geq 2$, wkt, Every integer $n \geq 2$ has a prime factor.

There fore,N is divisible by some prime pi,where $1 \leq i \leq n$.

Since pi|N and pi| $p_1 p_2 \cdots p_n \Rightarrow$ pi|$(N - p_1 p_2 \cdots p_n)$,

that is, pi|1, which is impossible.

Thus, our assumption is false, so there are infinitely many primes.

Greatest Common Divisor (GCD)

The greatest common divisor (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).

IMPORTANT RESULTS

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

- d|a and d|b and
- if d |a and d |b, then $d \leq d$, where d is also a positive integer. Thus, d = (a, b) if two conditions are satisfied:
- d must be a common factor of a and b.
- d must be the largest common factor of a and b; in other words, any other common factor d must be $\leq$ d.

For example, (12, 18) = 6, (12, 25) = 1, (11, 19) = 1, (−15, 25) = 5, and (3, 0) = 3.

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

SOLUTION

(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

9.Evaluate (2076,1776) or Find the gcd of 2076 and 1776.

SOL: Apply the division algorithm with 2076 (the larger of the two numbers) as the dividend and 1776 as the divisor:

Continue this procedure until a zero remainder is reached:

2076 = 1 . 1776 + 300

1776 = 5 . 300 + 276

300 = 1 .276 + 24

276 = 11 .24 + 12

24 = 2 . 12 + 0

(2076, 1776) = 12

10.Using the euclidean algorithm, express (4076, 1024) as a linear combination of 4076 and 1024.

SOLUTION

(4076, 1024) = 4 (find the gcd)

$4 = 1004 - 50 \cdot 20$

$= 1004 - 50(1024 - 1 \cdot 1004)$ (substitute for 20)

$= 51 \cdot 1004 - 50 \cdot 1024$

$= 51(4076 - 3 \cdot 1024) - 50 \cdot 1024$ (substitute for 1004)

$= 51 \cdot 4076 + (-203) \cdot 1024$

11.State and prove the EUCLID'S LEMMA.

STATEMENT:If p is a prime and p|ab, then p|a or p|b.

PROOF :Given. P is a prime

To Prove: Either p|a or p|b.

Suppose p doen't a factor of a. Then p and a are relatively prime, (p,a)=1

there are integers α and β such that $\alpha p+\beta a = 1$.

Multiply both sides of this equation by b; we get $\alpha pb + \beta ab = b$.

Since p|p and p|ab, p|($\alpha pb + \beta ab$)

that is,p|b($\alpha p + \beta a$) = p|b.(since$\alpha p+\beta a = 1$.)

12.State and prove the 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

First, we will show by strong induction that n either is a prime or can be expressed as a product of primes. Then we will establish the uniqueness of such a factorization.

Let P(n) denote the statement that n is a prime or can be expressed as a product of primes.

To show that P(n) is true for every integer $n \geq 2$:

Since 2 is a prime, clearly P(2) is true.

Now assume P(2),P(3),...,P(k) are true; that is, every integer 2 through k either is a prime or can be expressed as a product of primes.

If k + 1 is a prime, then P(k + 1) is true. So suppose k + 1 is composite.

Then k + 1 = ab for some integers a and b, where $1 < a, b < k + 1$.

By the inductive hypothesis, a and b either are primes or can be expressed as products of primes;

in any event, k +1 = ab can be expressed as a product of primes.

Thus, P(k +1) is also true. Thus, by strong induction, the result holds for every integer $n \geq 2$. 2.

To establish the uniqueness of the factorization:

Let n be a composite number with two factorizations into primes: $n = p_1p_2 \cdots p_r = q_1q_2 \cdots q_S$.

We will show that r = s and every pi equals some qj, where $1 \leq i, j \leq r$; that is, the primes q1, q2,...,qs are a permutation of the primes p1, p2,..., pr. Assume, for convenience, that $r \leq s$.

Since $p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$, $p_1 | q_1q_2 \cdots q_s$, by Corollary 3.9, p1 = qi for some i. Dividing both sides by p1, we get: $p_2 \cdots p_r = q_1q_2 \cdots q_{i-1}\, q_iq_{i+1} \cdots q_s$ Now p2 divides the RHS, p2 = qj for some j.

Cancel p2 from both sides: $p_3 \cdots p_r = q_1q_2 \cdots q_{i-1}\, q_iq_{i+1} \cdots q_{j-1}\, q_jq_{j+1}q_s$ Since $r \leq s$, continuing like this,

we can cancel every p with some qk. This yields a 1 on the LHS at the end. Then the RHS cannot be left with any primes,

since a product of primes can never yield a 1; thus, we must have exhausted all qk's by now. Therefore, r = s and hence the primes q1, q2,...,qs are the same as the primes p1, p2,..., pr in some order.

Thus, the factorization of n is unique, except for the order in which the primes are written.

13. Prove that the product of any two integers of the form 4n + 1 is also of the same form.

PROOF

Let a and b be any two integers of the form 4n + 1, say, a = 4 + 1 and b = 4m + 1 for some integers and m.

Then ab = (4 + 1)(4m + 1)

= 16m + 4 + 4m + 1

= 4(4m +1 + m) + 1

= 4k + 1 where k = 4m + + m is an integer

Thus, ab is also of the same form.

14.Prove thatthere are infinitely many primes of the form 4n + 3.

PROOF (by contradiction)

Suppose there are only finitely many primes of the form 4n+3,

say, $p_0, p_1, p_2,..., p_K$, where $p_0 = 3$.

Consider the positive integer $N = 4p_1 p_2 \cdots p_K + 3$. Clearly, $N > p_K$ and is also of the same form.

If N itself is a prime, then N would be larger than the largest prime pk of the form 4n + 3, which is a contradiction.

Suppose N is composite. Since N is odd, every factor of N is of the form 4n + 1 or 4n + 3. If every factor is of the form 4n + 1,we know that,The product of any two integers of the form 4n + 1 is also of the same form . Therefore would be of the same form. But, since N is of the form 4n + 3, at least one of the prime factors, say, p, must be of the form 4n + 3.

Case 1

Let $p = p_0 = 3$. Then 3|N, so 3|(N − 3) by Theorem 2.4; that is, 3|4p1p2 ⋯ pk. So, 3|2 or 3|pi, where $1 \leq i \leq k$, but both are impossible.

Case 2

Let $p = pi$, where $1 \leq i \leq k$. Then p|N and $p|4p_1 p_2 \cdots p_K$,

so $p|(N - 4p_1 p_2 \cdots p_K)$, that is, p|3, again a contradiction.

Both cases lead us to a contradiction, so our assumption must be false.

Thus, there is an infinite number of primes of the given form.

15.Every composite number n has a prime factor ≤ √n.

PROOF (by contradiction)

Because n is composite, there are positive integers a and b such that n = ab, where

$1 < a < n$ and $1 < b < n$. Suppose $a > \sqrt{n}$ and $b > \sqrt{n}$.

Then $n = ab > \sqrt{n} \cdot \sqrt{n} = n$,

which is impossible.

Therefore, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Since both a and b areintegers, it follows that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

We know that, every positive integer ≥ 2 has a prime factor.

Any such factor ofa or b is also a factor of $a \cdot b = n$,

so n must have a prime factor $\leq \sqrt{n}$.

16. Find the number of primes ≤ 100

SOLUTION

Here $n = 100$. Then $\pi(\sqrt{n}) = \pi(\sqrt{100}) = \pi(10) = 4$.

The four primes ≤ 10 are 2, 3, 5, and 7; ie p_1, p_2, p_3, and p_4, respectively.

$$\pi(100) = 100 - 1 + 4 - \left(\left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{7} \right\rfloor\right)$$
$$+ \left(\left\lfloor \frac{100}{2 \cdot 3} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{5 \cdot 7} \right\rfloor\right)$$
$$- \left(\left\lfloor \frac{100}{2 \cdot 3 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 3 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 5 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 5 \cdot 7} \right\rfloor\right)$$
$$+ \left\lfloor \frac{100}{2 \cdot 3 \cdot 5 \cdot 7} \right\rfloor$$

$$= 103 - (50 + 33 + 20 + 14) + (16 + 10 + 7 + 6 + 4 + 2)$$
$$- (3 + 2 + 1 + 0) + 0$$
$$= 25$$

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

PROOF

Consider the n consecutive integers $(n + 1)! + 2,(n + 1)! + 3,...,(n + 1)! + (n + 1)$, where $n \geq 1$.

Suppose $2 \leq k \leq n + 1$, then $k|(n + 1)!$, $k|k \Rightarrow k|[(n + 1)! + k]$, for every k.

Therefore, each of them is a composite number.

$\Rightarrow$ $|[(n + 1)! + k]$ is the n consecutive composite number

Thus, the n consecutive integers $(n+1)!+2,(n+1)!+3,...,(n+1)!+(n+1)$

are composites.

DEFINITION :Least Common Multiple

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

18.Using the canonical decompositions of 1050 and 2574, find their lcm.

SOLUTION:

Notice that $1050 = 2 \cdot 3 \cdot 5^2 \cdot 7$ and $2574 = 2 \cdot 3^2 \cdot 11 \cdot 13$. Therefore,

$$[1050, 574] = 2^{\max\{1,1\}} \cdot 3^{\max\{1,2\}} \cdot 5^{\max\{2,0\}} \cdot 7^{\max\{1,0\}} \cdot 11^{\max\{0,1\}} \cdot 13^{\max\{0,1\}}$$
$$= 2^1 \cdot 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^1 \cdot 13^1 = 450,450$$

19. Let a and b be positive integers. Then prove that $[a,b] = \frac{ab}{(a,b)}$

Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ be the canonical decompositions of a and b, respectively. Then

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

and

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

Therefore,

$$\begin{aligned}
(a, b) \cdot [a, b] &= p_1^{\min\{a_1, b_1\}} \cdots p_n^{\min\{a_n, b_n\}}, p_1^{\max\{a_1, b_1\}} \cdots p_n^{\max\{a_n, b} \\
&= p_1^{\min\{a_1, b_1\} + \max\{a_1, b_1\}} \cdots p_n^{\min\{a_n, b_n\} + \max\{a_n, b_n\}} \\
&= p_1^{a_1 + b_1} p_2^{a_2 + b_2} \cdots p_n^{a_n + b_n} \\
&= \left(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}\right)\left(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}\right) \\
&= ab
\end{aligned}$$

Thus,

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