DIVISION ALGORITHM

View the lecture on YouTube: https://youtu.be/TJGm1Af25S0

Well-ordering Principle

Every non-empty subset of Natural numbers has a least element.

The Division Algorithm

The division algorithm is a fine application of the well-ordering principle and is often employed to check the correctness of a division problem.

THEOREM 1: (The Division Algorithm) Let a be any integer and b a positive integer. Then there exist unique integers q and r such that $a = bq + r, where\ 0 \leq r < b$.

Proof: The proof consists of two parts.

Existence proof:

Consider the set $S = \{a - bn : n \in Z\ and\ a - bn \geq 0\}$.

Clearly, $S \subseteq W$. We shall show that S contains a least element.

First we will show that S is a non-empty subset of.

Case (i) Suppose $a \geq 0$. Then $a = a - b.0 \in S$, so S contains an element.

Case (ii) Suppose $a \leq 0$. Since $b \in Z^+, b \geq 1$. W

Then $ab \leq a \Rightarrow -ba \geq -a \Rightarrow a - ba \geq 0. i.e.\ a - ba \in S$.

In both cases, S contains at least one element. So, S is a non-empty set of W.

$\therefore$ By 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 $r < b$.

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 $a - bn\ and\ \geq 0$

$a - b(q + 1) \in S\ \ i.e. r - b \in S$

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 $a = bq + r, where\ 0 \leq r < b$. ----(1)

Uniqueness Proof:

Suppose $a = bq_1 + r_1, where\ 0 \leq r_1 < b$

Then $bq + r = bq_1 + r_1$ by (1)

$\Rightarrow (q - q_1)b = r_1 - r \ \Rightarrow b/r_1 - r$

$If\ r_1 - r \neq 0, then\ b/r_1 - r.$ Which is a contradiction. $(since\ |r_1 - r| < b)$

$\therefore\ r_1 - r = 0 \Rightarrow\ r_1 = r$

Hence $(q - q_1)b = 0 \Rightarrow q - q_1 = 0 \Rightarrow q_1 = q.$

$\therefore\ a = bq + r, where\ 0 \leq r < b$ is unique.

Hence the proof.

Example 1: Find the quotient q and the remainder r when

(i) 207 is divided by 15.

(ii) -23 is divided by 5.

Solution:

(i) 207 = 15.13 + 12; so q = 13 and r = 12.

(ii) -23 = 5. (-5) + 2; so q = -5 and r = 2.

The Pigeonhole Principle and the Division Algorithm

The pigeonhole principle is also known as the Dirichlet box principle after the German mathematician Gustav Peter Lejeune Dirichlet who used it extensively in his work on number theory. It can be applied to variety of situations.

Suppose m pigeons fly into n pigeonholes to roost, where $m > n$. What is your conclusion? Because there are more pigeons than pigeonholes, at least two pigeons must roost in the same pigeonhole; in other words, there must be a pigeonhole containing two or more pigeons.

THEOREM 2: (The Pigeonhole Principle) If m pigeons are assigned to n pigeonholes, where $m > n$, then at least two pigeons must occupy the same pigeonhole.

Proof: (By Contradiction)

Suppose the given conclusion is false; that is, no two pigeons occupy the same pigeonhole. Then every pigeon must occupy a distinct pigeonhole, so $n > m$, which is a contradiction. Thus, two or more pigeons must occupy some pigeonhole.

Example 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.

Solution:

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

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

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, $x - y\ is\ divisible\ by\ b$.

The Divisibility Relation

Suppose we let $r = 0$ in the division algorithm. Then $a = bq + 0 = bq$. We than say that b divides a, b is a factor of a, a is divisible by b, or a is a multiple of b, and write $b|a$. If b is not a factor of a, we write b∤a.

THEOREM 2: Let a and b be positive integers such that $a|b\ and\ b|a. Then\ a = b$.

Proof:

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

Claim: $a = b$

Since $a|b \Rightarrow b = aq, for\ some\ q \in Z$. ----------(1)

Also, $b|a \Rightarrow aq|a \Rightarrow q = 1$

Substitute in (1), we have $a = b$.

Hence the proof.

THEOREM 3: Let $a, b, c, \alpha\ and\ \beta$ be any integers. Then,

(i) If $a|b\ and\ b|c$, then $a|c$. (transitive property)

(ii) If $a|b\ and\ a|c$, then $a|(\alpha b + \beta c)$.

(iii) If $a|b, then\ a|bc$.

Proof:

(i) $a|b \Rightarrow b = q_1 a \Rightarrow c = q_2 b, where\ a \neq 0, b \neq 0\ in\ Z,\ q_1, q_2$ are some integers.

$\therefore c = q_2(q_1 a) = (q_1\ q_2)a \Rightarrow a|c$.