PROPERTIES OF NUMBERS:

$\boxed{\text{DIVISION}}$

$\boxed{\text{DIVISIBILITY}}$ $\boxed{m, n \in \mathbb{Z}}$

We say $\boxed{\text{m divides n}}$ or

$m \mid n$ $\boxed{\text{n is divisible by m}}$

SYMBOL

iff $\boxed{m \neq 0 \text{ and } n = mk, \text{ for some } k \in \mathbb{Z}}$

m is a $\boxed{\text{DIVISOR}}$ or $\boxed{\text{FACTOR}}$ of n

and n is $\boxed{\text{DIVISIBLE}}$ by m

we call $mk = n$ a $\boxed{\text{DECOMPOSITION}}$

or $\boxed{\text{FACTORIZATION}}$ of n

CLEARLY: k is ALSO a $\boxed{\text{DIVISOR}}$ of n

and is uniquely determined by m

$\boxed{\text{DIVISORS}}$ OCCUR in PAIRS $\boxed{(m, k)}$

SQUARE NUMBER

n is a square number iff divisors of n are $\boxed{(m, m)}$

i.e $\boxed{n = m^2}$ $\qquad n = m \cdot m$

FACT 1

$\boxed{\text{If } (m, k) \text{ is a divisor of } n \text{ so is } (-m, -k)}$ → associated divisor

Proof

$n = m \cdot k$, so $n = (-m)(-k) = mk$

Remark:

Each number has an obvious decomposition

$$c = 1 \cdot c = (-1)(-c)$$

FACT 1a

i.e ± 1 together with $\pm c$ are TRIVIAL DIVISORS of c

$(1, c) \quad (-1, -c)$

FACT 2

$$\boxed{\text{If } m \mid n \text{ and } n \mid m \text{, then } m, n \text{ are associated i.e. } m = \pm n}$$

Proof

$m \mid n$ i.e $n = m k_1$ $\quad k_1, k_2 \in \mathbb{Z}$

$n \mid m$ i.e $m = n k_2$

so $m = m k_1 k_2$ iff $k_1 = k_2 = 1$ and $m = n$

or $k_1 = k_2 = -1$, and $m = -n$.

FACT 3

$$\boxed{\text{IF } m \mid n_1 \text{ and } m \mid n_2 \text{ THEN } m \mid (n_1 \pm n_2)}$$

$m \mid n_1$ i.e $n_1 = m k_1$

$m \mid n_2$ i.e $n_2 = m k_2$, hence

$(n_1 \pm n_2) = m(k_1 \pm k_2)$ i.e

$m \mid (n_1 \pm n_2)$

FACT 9

$\boxed{\text{IF } m|n \text{ AND } n|k \text{, then } m|k}$

Proof

$m|n \equiv n = mk_1$
$n|k \equiv k = nk_2$
$\rightarrow k = mk_1k_2 \equiv m|k.$

IN MOST QUESTIONS regarding DIVISORS we ASSUME THAT $\boxed{n > 0}$ and that one ONLY CONSIDERS $\boxed{\text{POSITIVE DIVISORS } (m, k)}$

We look first at positive FACTORISATIONS and then we work out others.

$\boxed{\text{THE BOOK DEFINITION}}$ FOR $n, m \in \mathbb{Z}$

$m|n$ iff $m > 0$ and $n = mk$, for some $k \in \mathbb{Z}$

considers only positive m i.e divisors $\boxed{(m, k) \quad m > 0, \; k \in \mathbb{Z}}$

DEFINITION

PROPER DIVISORS of n :

all positive divisors, including 1 that are less than n

FACT 5

If (m, k) is a DIVISOR of n

THEN the factors m, k

can't be both $> \sqrt{n}$

$> \sqrt{n}$

Proof:

assume NOT: $m > \sqrt{n}$ and $k > \sqrt{n}$

then $m \cdot k > \sqrt{n} \cdot \sqrt{n} = n$

contradiction with $n = mk$.

Re-write FACT 5

If (m, k) is a divisor of n

then $m \leq \sqrt{n}$ ~~and~~ OR $k \leq \sqrt{n}$

Problem :

$\boxed{\text{Find all positive DIVISORS of } n = 60}$

By fact 5 the number of divisors $m \le \sqrt{n} = \sqrt{60}$ i.e

$\boxed{m < 8}$ $m \le \sqrt{60} < \sqrt{64} = 8$

Six PAIRS of DIVISORS

$$\boxed{\begin{array}{lll} (1, 60) & (3, 20) & (5, 12) \\ (2, 30) & (4, 15) & (6, 10) \end{array}}$$

$m = 1, 2, 3, 4, 5, 6$

DIVISION AND REMINDERS

Let $b \neq 0$, and $b \in \mathbb{Z}$.

Any $a \in \mathbb{Z}$ is either a multiple of b or fall between two consecutive multiples qb and $(q+1)b$ of b.

WE WRITE IT

$$\boxed{\begin{array}{l} a = qb + r \\ r = 0, 1, 2 \ldots \quad, |b|-1 \end{array}} \quad q \in \mathbb{Z}$$

r is called the least positive reminder or simply **THE REMINDER** of a by division with b,

q is the incomplete quotient or simply **THE QUOTIENT**

$$321 = \underset{q}{4} \cdot \overset{b}{74} + \underset{r}{25}, \quad 46 = \underset{q}{(-2)}\overset{b}{(-17)} + \underset{r}{12}$$

DIVISION and REMINDERS

$b \neq 0$, $a, b \in \mathbb{Z}$

$$\boxed{a = qb + r} \qquad 0 \leq r < |b|$$

$$q \in \mathbb{Z}$$

r - reminder of a by division with b

q - quotient

NOTE : Given $a, b \in \mathbb{Z}$, q and r are UNIQUELY DETERMINED and EACH INTEGER $a \in \mathbb{Z}$ can be written as

$$a = qb + r, \quad 0 \leq r < |b|$$

In particular any $n \in \mathbb{Z}$

$n = 2q$ or $n = 2q + 1$

EVEN ODD

THM The square of $n \in \mathbb{Z}$ is either DIVISIBLE by 4, or leaves the reminder 1 when divided by 4

Proof

(1) $n = 2q$, $n^2 = (2q)^2 = \underline{4}q^2$; (2) $n = 2q + 1$ $n^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$

DIVISION and REMINDERS

$b \neq 0$, $a, b \in \mathbb{Z}$

$$\boxed{a = qb + r}, \quad 0 \leq r < |b|, \quad q \in \mathbb{Z}$$

We re-write it

$$\boxed{\frac{a}{b} = q + \frac{r}{b}} \quad 0 \leq \frac{r}{b} < 1$$

FACT

q is the greatest INTEGER such that $q \leq \dfrac{a}{b}$

SPECIAL NOTATION

$$[q] = \frac{a}{b}$$ (OLD notation

NEW NOTATION after K.E IVERSON (1960)

* $\left\lfloor \frac{a}{b} \right\rfloor$ = greatest integer such that it is less or equal $\frac{a}{b}$

GENERAL DEFINITION

Book p67

FLOOR $\lfloor x \rfloor$ = the greatest integer q, $q \leq x$

$\lceil x \rceil$ = the least integer q, $q \geq x$

CEILING

DIVISION and REMINDERS

$\boxed{q = \lfloor \frac{a}{b} \rfloor}$ is the greatest integer q

$$q \leq \frac{a}{b} \qquad \text{(FLOOR)}$$

is also called

THE GREATEST INTEGER CONTAINED in $\frac{a}{b}$

EXAMPLES

$$\left\lfloor \frac{27}{5} \right\rfloor = 5, \quad \left\lfloor \frac{5}{3} \right\rfloor = 1, \quad \lfloor 2 \rfloor = 2, \quad \left\lfloor -\frac{1}{3} \right\rfloor = -1$$

$$\left\lfloor \frac{1}{3} \right\rfloor = 0$$

We EXTEND NOTATION TO REAL NUMBERS

DEF

$$x = q + y, \quad 0 \leq y < 1, \quad q \in \mathbb{Z}$$

$$x, y \in \mathbb{R} \qquad q = \lfloor x \rfloor$$

EXAMPLES

$$\lfloor \pi \rfloor = 3, \quad \lfloor e \rfloor = 2 \quad \left\lfloor \frac{\pi^2}{2} \right\rfloor = 4$$

MORE OF THIS in CHAPTER 3.

NUMBER SYSTEMS

REPRESENT:

$$\boxed{a = a_n b^n + a_{n-1} b^{n-1} + \dots a_1 b + a_0}$$

where $a_i \in \{0, 1, \dots b-1\}$

a on the BASE b

WRITE

$$\boxed{a = (a_n, a_{n-1}, \dots a_1, a_0)_b}$$

QUESTION ① how to find the representation on the base b

② How to pass from one base to the other.

OBSERVATION

① a_0 - is the REMINDER of a by division by b and

$a = b(a_n b^{n-1} + \dots a_1) + a_0$

$$\boxed{a = q_1 b + a_0}$$

where $\boxed{q_1 = a_n b^{n-1} + \dots a_2 b + a_1}$

$$\boxed{a = q_1 b + a_0}$$

$$q_1 = a_n b^{n-1} + \dots + a_2 b + a_1$$

~~POLYNOMIAL~~ ~~a~~ REPEAT

$$\boxed{q_1 = b q_2 + a_1}$$

a_1 is the reminder of q_1 by division by b

$$q_2 = a_n b^{n-2} + \dots + a_3 b + a_2$$

a_2 - is a reminder of q_2 by division by b

REPEAT TO FIND all $a_1 a_2 \dots a_n$!

a_i - is a reminder of q_i by division by b $\quad i = 1 .. n-1$

EXAMPLE: REPREZENT 1,749 in a system with base 7

$1{,}749 = \boxed{249} \cdot 7 + 6$

$249 = 35 \cdot 7 + 4$

$35 = \overset{a_n}{5} \cdot 7 + 0$

$$\boxed{1{,}749 = (5, 0, 4, 6)_7}$$

EXAMPLE

REPRESENT 19,151 to the base 12

$$19{,}151 = 1{,}595 \cdot 12 + 11 \qquad a_0 = 11$$

$$1{,}595 = 132 \cdot 12 + 11 \qquad a_1 = 11$$

$$132 = 11 \cdot 12 + 0 \qquad a_3 = 0$$

$$a_4 = 11$$

$$\boxed{19{,}151 = (11, 0, 11, 11)_{12}}$$

We evaluate $\boxed{a_0\, a_1 \ldots a_n}$ from the lowest UPWARD.

NOW let's evaluate $a_n, a_{n-1}, \ldots a_0$ DOWNWARD

In this case we have to determine the HIGHEST POWER of b such that b^n is less than a, while the next power b^{n+1} exceeds a.

We look for a division of a by b^n and

$$\boxed{a = a_n b^n + r_{n-1}}$$

$$r_{n-1} = a_{n-1} b^{n-1} + \cdots + a_0$$

We determine a_{n-1} from r_{n-1}

$$\boxed{r_{n-1} = a_{n-1} b^{n-1} + r_{n-2}}$$

$a_0 = r_{n-2}$

$$r_{n-2} = a_{n-2} b^{n-2} + \cdots + a_0$$

$$\boxed{r_{n-2} = a_{n-2} b^{n-2} + r_{n-3}}$$

etc.

EXAMPLE: Represent 1,832 to the base 7

FIRST: calculate powers of 7

7, $7^2 = 49$, $7^3 = 343$, $7^4 = 2{,}401$

$$\boxed{a = a_n b^n + r_{n-1}}$$

$$r_{n-1} = a_{n-1} b^{n-1} + \dots + a_0$$

$n = 3$

$$1{,}832 = \overset{a_n}{5} \cdot 7^3 + \underset{r_2}{117}$$

$$117 = \overset{a_{n-1}}{2} \cdot 7^2 + \underset{r_1}{19}$$

$$19 = \overset{a_{n-2}}{2} \cdot 7 + \underset{r_0 = a_0}{5}$$

$a_3 = 5$

$a_2 = 2$

$a_1 = 2$

$a_0 = 5$

$$\boxed{1{,}832 = (5, 2, 2, 5)_7}$$

why different bases! For example, division becomes simpler

$\frac{1}{3} = 0.3333\dots$ base 10

?

$\frac{1}{3} = (0,2)_6 = (0,4)_{12}$

LARGE BASES – short representations but MULTIPLICATION tables grow!

12×12 for base 12 60×60 for base 60!