imp: for remainder $r = a \bmod d$ always → write in sol
$a - d\lfloor a/d \rfloor$ * imp note for all quest. remainder cannot be negative

Date

$-11 \Rightarrow a$ (dividend
$3 \Rightarrow d$ (divisor).

$q = a \text{ div } d.$

$q = \lfloor -11/3 \rfloor$

$q = -4$

$r = a \bmod d$

$-11 = 3q + r.$

or $-11 \bmod 3$

$-11 = 3(-4) + r.$

$r = 1.$

$\therefore -11 = 3(-4) + 1$ Ans!

EXERCISE :- pg 281

Does 17 divides each of the following :-

(a) 68.

a divides b such that
a|b only when.
there exisits an integer
c to;
$ac = b.$

17 divides 68
because.

$17 \cdot 4 = 68.$

also 68/17 is an integer.

(b) 84

17 does not divide 84.
because there exisit no
value of c to satisfy.

$ac = b.$

or.

84/17 is not an integer.

(c) 357.

17 divides 357
because there exisit c
to satisfy.

$17 \cdot 21 = 357$

or 357/17 is an integer.

Date

Question no.2

Prove that if a is an integer other than 0 then.

(1) 1 divides a.

we know that

$n|m \Leftrightarrow (\exists q \in \mathbb{Z})$ such that $m = n.q$

here $m = q = a$
$n = 1$

$\therefore$ $a = 1.a$ proved

also $a/1$ is an integer.

(2) a divides 0;

$n|m \Leftrightarrow (\exists q \in Z)$ such that
$m = nq$.

here $0 = m = q$
$n = a$

$\therefore$ $0 = 0.a$ (proved!)

also $a/0$ is an integer.

Q no.3

Prove that part (ii) of theorem 1 is true.

Theorem 1.
part (ii).

if $a|b$, then $a|bc$ for all integers of c;

given: $a|b$
To proof: for all integers c $a|bc$

Prove:

$a|b$.
let d be an integer such that by the definition of division

$a.d = b$.

now multiply 'c' an integer on b.s.

$a.d.c = b.c$
$a(dc) = bc$

dc is also an integer as multiplied by d = integer and c = integer to form.

Date

hence by the definition of division it is proved.

$a|b$ where $(dc) \in \mathbb{Z}$ such that
$a(dc) = b.$

Question no. 4.
Prove part (iii) Theorem 1

Theorem 1
part (iii)

$a|b$ and $b|c$ then $a|c$:

given : $a|b$ & $b|c$
To proof : $a|c$

prove:
$a|b.$
then there exisit an integer d such that.

$a.d = b.$

also $b|c$
$b.f = c.$

Now combining both equs.

$(a.d)f = c$

$a(d.f) = c.$

where the product of two integers is another integer.

$d.f \in \mathbb{Z}$

$\therefore$ By the definition of division.

$a|c$ hence proved!

Question no. 5
Show that $a|b$, $b|a$ where a & b are integers, then $a=b$ or $a=-b$.

$a|b$
$\therefore a.c = b.$

$b|a$
$\because a = b.d$

combing:

$= b$ or $a = b.d$
$a = b(c)d = a(cd)$

Date

Now

$$a = a(cd)$$

By the identity property of multiplication, cd has to be = 1.

$$c = d = 1 \text{ or } c = d = -1$$

let these values of d on the equation.

$$a = b.d.$$

$$a = b(1)$$

$$a = (-1)b.$$

Thus we have shown as required!

Question no.6

Show that if a, b, c, d are integer, a ≠ 0 such that a|c and b|d then ab|cd.

a|c

then by the definition of division

$$a \cdot f = c. \qquad f \in \mathbb{Z}$$

also b|d.

then by the definition of division.

$$b \cdot g = d. \qquad g \in \mathbb{Z}$$

Multiplying both equations with each other.

$$(af)(b.g) = dc.$$

$$af\,bg = bc.$$

$$(ab)(fg) = cd.$$

since f and g ∈ ℤ then fg ∈ ℤ

ab|cd is proved by the definition of divides.

Date

Question no. 7

Show that if a, b, and c are integers, where $a \neq 0$ and $c \neq 0$ such that $ac \mid bc$ then $a \mid b$.

$ac \mid bc$ then there exisits an integer d such that

$$ac(d) = bc.$$

as given $c \neq 0$ we can divide c on b.s

$$b = ad.$$

then again by the definition of divides

$a \mid b$. where $d \in \mathbb{Z}$.

*(imp!)
Question no. 8

Prove or disapprove that if $a \mid bc$ where a, b, c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.

Given; a, b and c are $\mathbb{Z}^+$ with $a \mid bc$ and $a \neq 0$. The statement claims that $a \mid b$ or $a \mid c$.

Consider an example
4 divides 36 such that $36 = 4 \cdot 9$

also
6 divides 36 such that
$36 = 6 \cdot 6$.

But. 4 does not divide 6 as $6/4$ is not an integer.

Thus the statement is thus false when.

$a = 4$
$b = 6$
$c = 6$.

disproven!

*Imp Date

QUESTION NO. 9

Prove that a and b are integers and a divides b then b is even and a is odd.

n is even if and only if n is divisibly by 2 and if and only if there exist an integer K such that $n = 2K$.

n is odd if and only if there exist an integer k such that $n = 2k+1$.

To prove

$a|b$

then by the definition of divides.

$b = {}^{k}a$

when b is even, the proof is finished.

when b is odd, we require k and a both to be odd as product of 2 odd are odd

(but the product of an even integer is eve)

Thus we obtained that a is odd.

Since b is even or b is odd, we conclude that a is odd b is even.

*Imp

Question no. 10 :-

Prove that 'a' and 'b' are non zero $\mathbb{Z}^+$ a divides b, and a+b is odd, then a is odd.

By contradiction

$a|b$

then

$a \cdot q = b$.

Say

$a+b$.

then

$a+b = a + aq$

$= a(1+q)$

Now a is even so there is an integer k such that;

$a = 2k$.

Date

it implies

$a+b = 2k(1+q)$

where $k = (1+q)$

hence

$a+b$ is even.

which contradicts that $a+b$ is odd.

proved.

a cannot be even when $a+b$ is odd and $a|b$.

Question 11:- Imp

Prove that if a is an integer that is not divisible by 3, then $(a+1)(a+2)$ is divisible by 3.

By the division algorithm.

$a = 3q + r$. —(i)

three consts q & r with $0 \leq r < 3$ however '$r=0$' is not possible as a is not divisible by 3.

thus we have.

$r = 1$ or $r = 2$

$r = 1$

$(a+1)(a+2) = (3q+r+1)(3q+r+2)$

let $r = 1$;

$(3q+2)(3q+3)$ —(a)

$3(3q+2)(q+1)$

Since q is an integer. the $(3q+2)(q+1) \in \mathbb{Z}$.

and thus

$(a+1)(a+2) = 3(3q+2)q+1$ is divisible by 3.

Similarly for $r=2$;

just replace $r=2$ at point (a) and find result as accordingly.

Imp!

Date

Question no. 12.

Prove that if a is a positive integer, then 4 does not divide a^2+2.

Proof by Contradiction

lets say for the sake of contradiction.

4 divides a^2+2.

then a^2+2 is even.

* Since 2 is even and the sum of even and odd integer is odd then a^2 is even.

since the product of an odd no. $\mathbb{Z}$ with an odd no. $\mathbb{Z}$ is odd, then

square of an odd $\mathbb{Z}$ is also odd

$\therefore$ again a is an even integer.

then by the definition of divides.

$$a=2k.$$

$$a^2=(2k)^2$$

$$a^2=4k^2$$

Add 2 on b.s.

$$a^2+2=4k^2+2.$$

Note that 4 doesnot divide a^2+2.

$\therefore$

the assumption is incorrect hence proved!

Question no. 13.

What are the quotients and remainders

(a) 19 divided by 7.

$a=19$

$d=7$

$19=q(7)+r.$

$q=\lfloor 19/7 \rfloor$

$q=2(7)+5.$

Date

(f) 0 is divided by 19.

$0 = q(19) + r$

$q = \lfloor 0/19 \rfloor =$ a div d.

$q = (0)$

$r = 0.$ $\Rightarrow$ a mod d.

$0 = q(19) + r.$

(f)* 3 is divided by 5?

$3 = 5q + r.$

$q = 3 \text{ div } 5.$

$q = \lfloor 0.16 \rfloor$

$$\begin{array}{r} .16 \\ 3\overline{)\,50} \\ \underline{48} \\ 2 \end{array}$$

$q = 0.$

remainder. = a mod d

= 3 mod 5.

$\Rightarrow 3$

$3 = 5(0) + 3$ proved!

(g) −1 divided by 3?

$(-1) = 3(q) + r.$

$q = \lfloor -1/3 \rfloor$

$q = -01$

$r = -1 \text{ mod } 3.$

$$\begin{array}{r} -2 \\ -1\overline{)\,3} \\ \underline{\mp 2} \\ 1. \end{array}$$

$r = 2.$

$(-1) = 3(-1) + 2.$

proved!

(h) 4 is divided by 1?

$4 = (1)q + r.$

$q = 4 \text{ div } 1$ $\quad 4\overline{)\,1}$

$q = \lfloor 4/1 \rfloor$

$q = 4$

$R = 0.$

$4 = (1)(4) + 0.$

proved!

Date

Q no. 14:
Quotient = ?
Remainder = ?

(f) 0 is divided by 17?

$0 = 17q + r$

$q = \lfloor 0/17 \rfloor$

$q = 0$
$r = 0$.

(g) 1,234,567 is divided by 1001.

$1234567 = 1001q + r$.

$q = \lfloor 1234567/1001 \rfloor$

$q \Rightarrow 1233$

$r = 334$.

(h) -100 is divided by 101?

$-100 = 101q + r$.
$q = \lfloor -100/101 \rfloor$
$q = -1$; $r = 1$

15, 16, 10, 11
19, 20, 21, 22, 23, 24
26, 27, 28, 29
30, 31, 36, 37
38, 39, 40

Imp!
Q no 15:-

What time does a 12-hour clock read?

(a) 80 hours after it reads 11:00?

a 12 hour clock will show the same time after each 12 hour interval.

let $80 = a$
$12 = d$.

$a = 80 \Rightarrow 72 + 8$.

$\Rightarrow (12)6 + 8$

$q = 6$.
$r = 8$;

$0 \leq 8 < 12$.

$80 \bmod 12 = 8$.

The remainder is 8 thus 80 hours after 11:00 is same as 8 hours after it reads 11 ∴ it will read 7 o'clock.

Date

(b) 40 hour before 12:00?

$a = 40.$
$d = 12$ (12 hour clock)

$40 = (12)q + r.$

$q = \lfloor 40/12 \rfloor$

$q = 3.$

$r = 4.$

Thus 40 hours before 12 is same as 4 hours before 12 thus it is 8 o'clock.

(c) 100 hours after it reads 6:00?

$a = 100$
$d = 12$ (12 hour clock)

$100 = q(12) + r$

$q = 8(12) + 4.$

Thus 100 hours after 6 is as same as 4 hours after 6 which is 10 o'clock.

Question no. 6:-

What does the 24 hour clock read.

(a) 100 hours after it reads 2:00?

$a = 100$
$d = 12 + 12 = 24.$ ★

$a = dq + r.$

$100 = (24)q + r$

$q = \lfloor 100/24 \rfloor$

$q = 4$

$100 = (24)(4) + 4.$

$R = 4$

∴ it is same as ~~6~~ 4 hours after 2:00 i.e 6 o'clock.

Date

(b) 45 hours before it reads 12:00.

$a = 45$
$d = 24$

$45 = 24(q) + r.$

$q = \lfloor 45/24 \rfloor$

$q = 1.$
$r = 20 + 1 = 21.$

$\therefore$ it is the same time as before/after 21 hours from 12:00.
i.e 3'oclock in noon
15:00hrs.

(c) 168 hours after it reads 19:00?

$a = 168$
$d = 24$

$168 = (24)q + r.$
$q = 4 + 3 \Rightarrow 7$
$r = 0.$
$\Rightarrow$ 19:00 ans!

Question 19.

show that if 'a' and 'd' are $\mathbb{Z}^+$ then $(-a)$ div d = $-a$ div d if and only if d divides a.

generally
let $a = 6$ and $d = 3$.

a div d = $6/3 \Rightarrow 2$.

①
$-a = -6$
$\Rightarrow$ $(-a)$ div $d \Rightarrow -6$ div 3
$\Rightarrow -2$

given that
———x———

$(-a)$ div d = $-a$ div d.

let again

$a = 7$ and $d = 3$.

a div d = 7 divided by 3
= 2 (remainder = 1)
——①

$-a = -7$
$\Rightarrow (-a)$ div $3 \Rightarrow -3$.
——②

Date

if ① is

$a \operatorname{div} d$

$- (a \operatorname{div} d)$

$\Rightarrow -2$ —— (a)

and ② is

$(-a) \operatorname{div} d$

$\Rightarrow -3$ —— (b)

thus $a \neq b$ and

$-a \operatorname{div} d = (-a) \operatorname{div} d$

if and only if d divides a.

proved.

Q no. 20

Prove or disprove that if 'a', 'b' and 'd' are integers with $d > 0$ then $(a+b) \operatorname{div} d = a \operatorname{div} d + b \operatorname{div} d$.

Counter example solution.

let $a = 3$
$b = 3$
$d = 2$.

Now.

$a \operatorname{div} d = \lfloor 3/2 \rfloor = 1$

$b \operatorname{div} d = \lfloor 3/2 \rfloor = 1$.

also

$(a+b) \operatorname{div} d \Rightarrow (3+3) \operatorname{div} 2$.

$\Rightarrow 6 \operatorname{div} 2$

$\Rightarrow 3$

we note that.

$a \operatorname{div} d + b \operatorname{div} d = 1+1 = 2$.

while

$(a+b) \operatorname{div} d = 3$

thus disprove (not equal)

Date

24. Show that if $a \in \mathbb{Z}$ and $d \in \mathbb{Z} > 1$. then 'q' and r are equal to $\lfloor a/d \rfloor$ & $a - d\lfloor a/d \rfloor$ respectively.

By the division algorithm we know that:

$$a = qd + r.$$

where $0 \leq r < d$

a = dividend

q = quotient

r = remainder

d = divisor.

$$\frac{a}{d} = q + \frac{r}{d}$$

as we know from $0 \leq r < d$.

then; $r < d$ and $\frac{r}{d} < 1$.

$\therefore$

$$\lfloor a/d \rfloor = \left\lfloor q + \frac{r}{d} \right\rfloor \Rightarrow q$$

Similarly for the remainder we would use the division algorithm

$$r = a - qd.$$

substituting q

$$r = a - d\lfloor a/d \rfloor$$

hence proved!

Question no. 26:-

(C) $-101 \bmod 13$.

$a = -101$

$d = 13$

$-101 = 13q + r.$

$q = \lfloor -101/13 \rfloor$

$q = -8.$

$r = 3.$

$-101 \bmod 13 = 3.$

Date

(d) 199 mod 19.

$a = 199$
$d = 19$

$a = dq + r$ → division algorithm.

$199 = 19q + r$

$q = \lfloor 199/19 \rfloor$

$q = 10$

$r = a - d\lfloor a/d \rfloor$
⇒ 9.

∴ 199 mod 19 = 9.

Qno.25(+)2 :-
Evaluate.

(c) 155 mod 19.

$a = 155$
$d = 19$.

$a = dq + r \Rightarrow 155 = 19q + r$.

$q = \lfloor 155/19 \rfloor = 8$
$r = 3$ (by $a - d\lfloor a/d \rfloor$)

(d) −221 mod 23.

$-221 = 23q + r$.

$q = \lfloor -221/23 \rfloor$

$q = -10$

$r = a - d\lfloor a/d \rfloor$.

$r = 9$.

−221 mod 23 = 9

Qno.28.
a div m & a mod m.

(c) $a = 10299$, $m = 999$.

① $\lfloor a/d \rfloor = q = \lfloor 10299/999 \rfloor$ ($d = m$)

$= 10$

② $r = a - d\lfloor a/d \rfloor \Rightarrow 309$.

(d) $a = 123456$ $m = 1001$.
$a \text{ div } m = \lfloor a/m \rfloor = \lfloor 123456/1001 \rfloor$
$= 123$
$a \bmod m = a - d\lfloor a/m \rfloor \Rightarrow 333$.

Date

Qno.29:-

a div m.

a mod m.

(c)

$a = -10101$

$m = 333.$

$a \text{ div } m = \lfloor a/d \rfloor$

$= \lfloor -10101/333 \rfloor$

$= -31$

$a \text{ mod } m = 222.$

(d) $a = -765432$

$m = 38271.$

$a \text{ div } m = \lfloor a/m \rfloor$

$= \lfloor -765432/38271 \rfloor$

$= -21$

$a \text{ mod } m = 38259.$

Question 36.

(a)

$(177 \text{ mod } 31 + 270 \text{ mod } 31)$
$\text{mod } 31.$

$177 \text{ mod } 31.$

$a \text{ mod } d.$

$\Rightarrow a - d \lfloor a/d \rfloor$

$\Rightarrow 177 - 31 \lfloor 177/31 \rfloor.$

$\Rightarrow 22.$

$270 \text{ mod } 31$

$\Rightarrow 270 - 31 \lfloor 270/31 \rfloor$

$\Rightarrow 22.$

$(22 + 22) \text{ mod } 31$

$44 \text{ mod } 31$

$\Rightarrow 44 - 31 \lfloor 44/31 \rfloor$

$\Rightarrow 13$ Ans!

(b) $(177 \text{ mod } 31 \cdot 270 \text{ mod } 31)$
$\text{mod } 31$

follow same steps as before.

$(22 \cdot 22) \text{ mod } 31$

$484 \text{ mod } 31$

$\Rightarrow 19$ ans!

Date

Question no. 37.

Similar Question.

Question no. 38.

(c) $(7^3 \bmod 23)^{\wedge 2} \bmod 31$

$7^3 = 343$.

$343 \bmod 23$

$343 - 23\lfloor 343/23 \rfloor$

$(21)^2 \bmod 31$

$441 \bmod 31$

$441 - 31\lfloor 441/31 \rfloor = 7$.

Question no. 39.

(d) $(893 \bmod 79)^4 \bmod 26$

$(704969 \bmod 79)^4$

$704969 - 79\lfloor 8923 \rfloor$

$\Rightarrow (52)^4 \bmod 26$

$\Rightarrow$

$7311616 \bmod 26$.

$7311616 - 26(281216)$

$\Rightarrow 0$.

Q no. 23:-

show that n and k are positive integers then

$\lceil n/k \rceil = \lfloor (n-1)/k \rfloor + 1$.

let $\left.\begin{aligned} n &= 2 \\ k &= 3 \end{aligned}\right\} \mathbb{Z}^+$.

R.H.S

$\lceil n/k \rceil \Rightarrow 2/3 \Rightarrow 1$

L.H.S

$\lfloor (2-1)_3 \rfloor + 1$

$0 + 1 = 1$

hence

L.H.S = R.H.S proved.