PROJECTED WRITTEN NOTES FROM the M325K LECTURE ON THURSDAY, FEBRUARY 8, 2024, ON SEC 4.4 – DIVISIBILITY, the QUOTIENT-REMAINDER THEOREM, and the $\langle n \bmod d \rangle$ function

CLASS #8

Recall the definition of "d divides n" $(d \mid n)$:

Let n and d be integers.

"d divides n" ("$d \mid n$") [also "n is divisible by d"]

if and only if

there exists an integer k such that $n = dk$.

$3 \mid 12$ since $12 = 3 \cdot 4$.

Recall:

Theorem 4.3.1: For all positive integers a and b,

if $a \mid b$, then $a \leq b$.

Learn this theorem by NAME "Theorem 4.3.1"

Theorem 4.3.3 (Divisibility is Transitive)

For all integers a, b, c,
if $a|b$ and $b|c$, then $a|c$.

Proof: Let a, b, c be any integers.
Suppose $a|b$ and $b|c$. [WTS: $a|c$]

Since $a|b$, then exists an integer k
such that $b = ak$, by defn of "divides".

Also, for some integer l, $c = bl$
by defn of "divides".

$\therefore c = (ak)l$, by substitution
$= a(kl)$ by R.O.A.

Let $t = kl$, and t is an integer since
sums and products of integers are integers.

$\therefore c = at$, by subst, and t is an integer.

$\therefore a|c$, by defn of "divides".

$\therefore$ For all integers a, b, c, if $a|b$ and $b|c$, then $a|c$,
by Direct Proof. QED.

WORKSPACE

$a|b \rightarrow b = ak$

$b|c \rightarrow c = bl$

$c = (ak)l$

$c = a(kl)$

$c = at$

$\therefore a|c$

Theorem 4.3.4: For each integer $n > 1$,

there exists an integer p such that $p \mid n$.

Proof: (Shown Later)

Theorem (Can be applied without citation)

For positive integers a and b,

$a \nmid b$ if and only if $\frac{b}{a}$ is not an integer.

EXAMPLE: Prove that $5 \nmid 13$

Proof: $\frac{13}{5} = 2\frac{3}{5}$, so, $2 < \frac{13}{5} < 3$.

$\therefore \frac{13}{5}$ is not an integer since there are no integers between 2 and 3. $\frac{13}{5}$ is not an integer.

$\therefore 5 \nmid 13$, since $\frac{13}{5}$ is not an integer.

A Theorem is a statement with a proof.

You can apply theorem statements as justifications in the proofs you write — some, but not all.

A student asked me, "What theorems or principles can we use in writing proofs?"

My Policy: When you are writing a proof, you can use any theorem proved in class earlier or was proved in the book in the current reading or from earlier readings.

You can also use the results of previous homework assignment or in any problem set earlier in the book.

Another Theorem

Theorem 4.4.1: The Quotient-Remainder (Q-R) Theorem.

For every integer n and every POSITIVE integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

EXAMPLE: Apply the Q-R Theorem with

$n = -60$ and $d = 9$.

Soln: We seek q and r such that $n = dq + r$

$$-60 = 9q + r$$
$$n = 9q + r.$$

Let $q = -10$, then $9q = -90$ and

$-60 = -90 + 30$, so let $r = 30$.

with $q = -10$ and $r = 30$,

$dq + r = 9(-10) + 30 = -90 + 30 = -60 = n$.

But! $q = -10$ and $r = 30$ are not the unique integers from the Q-R Theorem,

Because, we must also have that $0 \le r < d$,

but "$0 \le 30 < 9$" is False.

In fact, with $q = -7$ and $r = 3$,

we have that

$dq + r = 9(-7) + 3 = -63 + 3 = -60 = n$

and $0 \le 3 < 9$

$0 \le r < d$

So, $q = -7$ and $r = 3$ are the unique q and r from the Q-R theorem.

EXAMPLE (FINDING q and r when n is Positive)

Let $n = 85$ and let $d = 7$

Use the division algorithm: $d \overline{)n}$ (q on top, r at the footer) $\Rightarrow n = dq + r$

$$\begin{array}{r} 12 \\ 7\overline{)85} \\ \underline{7} \\ 15 \\ \underline{14} \\ 1 \end{array}$$

$q = 12$, $r = 1$.

$85 = 7 \times 12 + 1$ and $0 \leq 1 < 7$

Definitions of the "mod" and "div" functions of n and d.

Given an integer n and a positive integer d,

the Q-R Theorem gives us unique integers q and r such that $n = dq + r$ and $0 \le r < d$.

We define "$(n \bmod d)$" to be r.

We define "$(n \operatorname{div} d)$" to be q.

$(n \bmod d) = r$ and $(n \operatorname{div} d) = q$.

Problem: Determine $(23 \bmod 4)$ and $(23 \operatorname{div} 4)$

$(n \bmod d)$ and $(n \operatorname{div} d)$

Here $n = 23$, $d = 4$.

Step 1: Find the unique q and r from the Q-R Theorem:

$q = 5$, $r = 3$

$23 = 4 \times 5 + 3$ and $0 \le 3 < 4$.

$n = dq + r$ $\quad 0 \le r < d$.

Step 2: Apply defns:

$(23 \bmod 4) = 3$ and $(23 \operatorname{div} 4) = 5$.

Problem: Find $(-29 \bmod 7)$

$(n \bmod d)$ $\quad n = -29$, $d = 7$

$-29 = 7 \times (-5) + 6$ and $0 \leq 6 < 7$

$-29 = -35 + 6$

$q = -5$ and $r = 6$ are the unique q and r from the Q-R theorem.

$\therefore (-29 \bmod 7) = 6$, by def'n of "$(n \bmod d)$".

In this class, always write "$(n \bmod d)$" using parentheses.

Don't write "$16 \bmod 5 = 1$"

Instead write "$(16 \bmod 5) = 1$" with parentheses!

EXAMPLE PROOFS INVOLVING THE (n mod d)-function

The following statements are proved in this handout:

(1) To Prove: $(67 \bmod 9) = 4$

(2) ~~To Prove: $(-28 \bmod 5) = 2$~~

(3) To Prove: For every integer b,
if $(b \bmod 16) = 10$, then $(46 \bmod 16) = 8$.

(4) To Prove: ~~For all integers c and d,~~
~~if $(c \bmod 8) = 5$ and $(d \bmod 8) = 7$,~~
~~then $(cd \bmod 8) = 3$.~~

---

(1) To Prove: $(67 \bmod 9) = 4$.

Proof: By the Quotient-Remainder (Q-R) theorem, there exist unique integers q and r such that $67 = 9q + r$ and $0 \leq r < 9$.

Also, by the definition of $(n \bmod d)$, $(67 \bmod 9) = r$.

Now, $67 = 9 \times 7 + 4$ and $0 \leq 4 < 9$.

So, by the uniqueness of q and r, $q = 7$ and $r = 4$.

∴ By substitution, $(67 \bmod 9) = 4$.

QED.

(2) To Prove: $(-28 \bmod 5) = 2$

Proof: By the Q-R Theorem, there exist unique integers q and r such that $-28 = 5q + r$ and $0 \leq r < 5$.

By definition of $(n \bmod d)$, $(-28 \bmod 5) = r$.

Now, $-28 = 5 \times (-6) + 2$ and $0 \leq 2 < 5$.

So, by the uniqueness of q and r, $q = -6$ and $r = 2$.

∴ By substitution, $(-28 \bmod 5) = 2$.

QED.

---

(3) To Prove: For every integer b, if $(b \bmod 16) = 10$, then $(4b \bmod 16) = 8$.

Proof: Let b be any integer such that $(b \bmod 16) = 10$.

[N.T.S: $(4b \bmod 16) = 8$].

By the Q-R Theorem, there exist unique integers q_1, r_1 and q_2, r_2 such that $b = 16q_1 + r_1$ and $0 \leq r_1 < 16$ and $4b = 16q_2 + r_2$ and $0 \leq r_2 < 16$.

By definition of $(n \bmod d)$, $(b \bmod 16) = r_1$ and $(4b \bmod 16) = r_2$.

Since $(b \bmod 16) = 10$, $r_1 = 10$ and $b = 16q_1 + 10$, by substitution.

[Proof of (3) continued]

$\therefore 4b = 4(16q_1 + 10)$, by substitution

$= 64q_1 + 40$

$= 16(4q_1) + 16 \times 2 + 8$

$= 16(4q_1 + 2) + 8$, by Rules of Algebra.

Let $t = 4q_1 + 2$. Then, t is an integer since sums and products of integers are integers.

$\therefore 4b = 16t + 8$, by substitution.

$\therefore 4b = 16t + 8$ and $0 \leq 8 < 16$.

By the uniqueness of q_2 and r_2, $q_2 = t$ and $r_2 = 8$.

As shown above, $(4b \bmod 16) = r_2$.

$\therefore (4b \bmod 16) = 8$, by substitution.

$\therefore$ For every integer b, if $(b \bmod 16) = 10$, Then $(4b \bmod 16) = 8$, by Direct Proof.

QED.

---

(4): To Prove: For all integers c and d, if $(c \bmod 8) = 5$ and $(d \bmod 8) = 7$, then $(cd \bmod 8) = 3$.

Proof: Let c and d be any integers.

Suppose $(c \bmod 8) = 5$ and $(d \bmod 8) = 7$. [Suppose the IF-part!]

[N.T.S.: $(cd \bmod 8) = 3$]

(Continued on the next page)