mod Example (1)

$25 \bmod 4 = 1$

$$
\begin{array}{r}
6 \\
4\,\overline{)\,25} \\
\underline{24} \\
1
\end{array}
$$

$25 \bmod 5 = 0$

$$
\begin{array}{r}
5 \\
5\,\overline{)\,25} \\
\underline{25} \\
0
\end{array}
$$

$271 \bmod 5 = 1$

$$
\begin{array}{r}
54 \\
5\,\overline{)\,271} \\
\underline{25} \\
21 \\
\underline{20} \\
1
\end{array}
$$

mod Example (2)

$m = nq + r$

* $25 \bmod 4 = 1$ because

$25 = 4 \cdot 6 + 1$, and

$25 = 4 \cdot q + r$ cannot be satisfied

for $0 \le r < 1$, i.e. $r = 0$

* $-25 \bmod 4 = 3$ because

$-25 = 4 \cdot (-7) + 3$ and

$-25 = 4 \cdot q + r$ cannot be satisfied

for $0 \le r < 3$,

i.e. $r = 0, 1, 2$

mod Example (3)

$21 \bmod 9 = 3$ $\qquad$ $38 \bmod 9 = 2$

$(21 \cdot 38) \bmod 9 = 798 \bmod 9 = 6$

so

$(21 \cdot 28) \bmod 9 = (21 \bmod 9) \cdot (38 \bmod 9) \quad (*)$

$(21 + 38) \bmod 9 = 59 \bmod 9 = 5$

So

$(21+38) \bmod 9 = (21 \bmod 9) + (38 \bmod 9) \quad (**)$

(*), (**) true in general?

True in General?

$$(ab) \bmod n = (a \bmod n) \cdot (b \bmod n) \quad (*)$$

$$(a+b) \bmod n = (a \bmod n) + (b \bmod n) \quad (**)$$

NO! Counter example

$$\overbrace{(2 \cdot 8) \bmod 9 \neq (2 \bmod 9) \cdot (8 \bmod 9)}$$

$$\quad 7 \qquad\qquad\qquad 2 \cdot 8$$

$$\qquad\qquad\qquad\qquad 16$$

Note: equality holds if $16 \rightarrow 16 \bmod 9$

$$(2+8) \bmod 9 \neq (2 \bmod 9) + (8 \bmod 9)$$

$$1 \qquad\qquad\qquad 10$$

Note: equality holds if $10 \rightarrow 10 \bmod 9$

$(*)$, $(**)$ true after modifications

Examples for Lemm 2.2

$25 \bmod 4 = 1$

$(25 + 2\cdot 4) \bmod 4 = 33 \bmod 4 = 1$

$(25 - 3\cdot 4) \bmod 4 = 13 \bmod 4 = 1$

proof of Lemm 2.2

* By Euclid's Division theorem,

  Exist unique q, r $(0 \le r < n)$ s.t.

$$i = n \cdot q + r \qquad (*)$$

* By definition of mod,

$$i \bmod n = r$$

* Similarly, exists unique

q', r' $(0 \le r' < n)$ s.t.

$$i + kn = n \cdot q' + r' \quad (**)$$

* By definition of mod,

$$(i + kn) \bmod n = r'$$

* From (*) we get

$$i + kn = n \cdot (q + k) + r \quad (***)$$

$$0 \le r < n$$

* Because of Division Theorem,

$$r' = r.$$

* That is

$$i \bmod n = (i + kn) \bmod n$$

Proved.

Lemma 2.3

$$(i+j) \bmod n = \big((i \bmod n) + (j \bmod n)\big) \bmod n$$

$$(i \cdot j) \bmod n = \big((i \bmod n) \cdot (j \bmod m)\big) \bmod n$$

<u>proof</u>

$$(i+j) \bmod n$$

$$= (i + (j \bmod n)) \bmod n$$

$$= ((i \bmod n) + (j \bmod n)) \bmod n$$

$$\boxed{i+j = i + (j \bmod n) + kn \quad \text{for some } k}$$

$$2 + 25 = 2 + \underbrace{(25 \bmod 4)}_{1} + 6 \cdot 4$$

$(i \cdot j) \bmod n$

$= (i \cdot (j \bmod n)) \bmod n$

$= ((i \bmod n) \cdot (j \bmod n)) \bmod n$

$\boxed{i \cdot j = i \cdot (j \bmod n) + k' n \text{ for some } k'}$

proved.

$$\underset{50}{2 \cdot 25} = 2 \cdot \underset{1}{(25 \bmod 4)} + 12 \cdot 4$$