5. d). $(\cancel{2^1} - \underbrace{2^0}_{}) + (\cancel{2^2} - \cancel{2^1}) + (\cancel{2^3} - \cancel{2^2}) + \cancel{\cdots} + (\underbrace{2^{10}}_{} - \cancel{2^9})$

$= 2^{10} - 2^0$

$= 1024 - 1 = 1023$

Chapter 4.

§4.1 Divisibility and Modular Arithmetic

1. Division.

Def. If $a, b \in \mathbb{Z}$ with $a \neq 0$, then we can say that a divides b. if there is an integer c s.t $b = ac$ or equivalently, if $\frac{b}{a}$ is an integer when a divides b we say that a is a factor or divisor of b, and b is a multiple of a. $a | b \Rightarrow \exists c \ (ac = b)$

Ex. $2 | 10 \Rightarrow 2 \cdot 5 = 10 \Rightarrow 2 | 10$ b/c $\frac{10}{2} = 5 \in \mathbb{Z}$

$3 | 7 \Rightarrow 3(\ \ ) = 7 \Rightarrow 3 \nmid 7$ b/c $\frac{7}{3}$ is not an integer.

Theorem 1. let $a, b, c \in \mathbb{Z}$, where $a \neq 0$, then

1) if $a|b$ and $a|c$, then $\boxed{a | (b+c)}$

Ex. $2 | 10$, $2 | 18 \Rightarrow 2 | ((10+18) \Rightarrow 2 | 28 \Rightarrow 28 = 2\underset{\in \mathbb{Z}}{\boxed{(14)}}$

2) if $a|b$, then $a|bc$ for all integer c

Ex. $2 | 10$, $2 | 10 \cdot 5 \Rightarrow 2 | 50$ ✓

3) if $a|b$ and $b|c$, then $a|c$.

Ex. $2 | 10$, $10 | 100$, $\Rightarrow$ $2 | 100$

Pf. 1) if $a|b$ and $a|c$

by definition: if $a|b$, then $b = a \cdot k$, $k \in \mathbb{Z}$

if $a|c$, then $c = a \cdot p$, $p \in \mathbb{Z}$

$b + c = ak + ap = \underline{a} \cdot (\underline{k+p})$

$k \in \mathbb{Z}$, $p \in \mathbb{Z} \Rightarrow k + p \in \mathbb{Z}$

let $k + p = M$

$b + c = a \cdot M$ $M \in \mathbb{Z} \Rightarrow$ by definition, $a | (b+c)$. ∎

2). if $a|b$, $b = a \cdot k$ $k \in \mathbb{Z}$ (by def.)

$bc = ak \cdot c = a(kc)$ $k \in \mathbb{Z}, c \in \mathbb{Z} \Rightarrow kc \in \mathbb{Z}$

by def. $a | (bc)$. ▨.

3). if $a|b$ and $\underline{b|c} \Rightarrow \frac{c}{b}$

by def. $b = \underbrace{a \cdot k}$ $k \in \mathbb{Z}$ $c = b \cdot p$ $p \in \mathbb{Z}$

$c = a(k \cdot p)$ $k, p \in \mathbb{Z}$, $kp \in \mathbb{Z}$

by def. $a | c$. ▨.

2. The Division Algorithm.

Theorem 2. let a be an integer and d a positive integer. Then there are unique integers q and r with $0 \le r < d$ s.t $a = d \cdot q + r$

d = divisor
q = quotient
r = remainder (can't be negative!)
a = dividend.

Notation: $q = a \text{ div } d$ $r = a \text{ mod } d$

Ex. 101 is divided by 11

101 div 11 = 9 ⇒ quotient

101 mod 11 = 2 ⇒ remainder.

$$\begin{array}{r} 9 \\ 11 \overline{)101} \\ 99 \\ \hline 2 \end{array}$$

Theorem 2: $101 = 11 \times 9 + 2$

3. Modular Arithmetic

Def. If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a is congruent to b modulo m if m divides $a-b$.

Notation: $a \equiv b \pmod{m} \Rightarrow m | (a-b)$

Ex. $11 \equiv 5 \pmod{3} \Rightarrow 3 | (11-5) \Rightarrow 3 | 6 \Rightarrow 6 = 3(2)$ ✓

$17 \not\equiv 4 \pmod 5 \Rightarrow 5 \nmid (17-4) \Rightarrow 5 \nmid 13 \Rightarrow 13 \not\equiv 5$ (?)

Theorem 3. let $a, b \in \mathbb{Z}$, and let $m \in \mathbb{Z}^+$, then $a \equiv b \pmod m$ $\boxed{\text{iff}}$ $\underline{a \bmod m = b \bmod m}$

Ex. $27 \equiv 18 \pmod 9 \Rightarrow 27 \bmod 9 = 0 = 18 \bmod 9$ ✓

$6 \overline{)35}$ 5, 30, 5

$35 \bmod 6 = 5 \neq 9 \bmod 6 = 3$ $\Rightarrow$ $\underbrace{35 \not\equiv 9 \pmod 6}_{(35-9)=26}$ $6 \nmid 26$

Pf. $\longrightarrow$ if $a \equiv b \pmod m$ then $a \bmod m = b \bmod m$

by definition of congruent: $m \mid (a-b)$ $\Rightarrow$ by def of divisibility $(a-b) = m \cdot k$, $k \in \mathbb{Z}$

$a = b + mk$

$a \bmod m = (b+mk) \bmod m$

$= b$

$$\frac{b+mk}{m} = \underbrace{\boxed{\frac{b}{m}} + \boxed{\frac{mk}{m}}}$$

$\uparrow r = b$ $\uparrow r = 0$

Ex. $\frac{3}{5}$ $5 \overline{)3}$ 0, 0, 3

$b \bmod m = b$

$\boxed{b > m.}$ $a \bmod m$

$= \frac{b + \cancel{mk}}{\cancel{m}}$

$= b \bmod m$

$a \bmod m = b \bmod m.$

$\leftarrow$ if $a \bmod m = b \bmod m$ then $\underbrace{a \equiv b \pmod m}_{\text{by def.}}$ $m \mid (a-b) \Rightarrow \underline{a-b} = \underline{m \cdot k}$

let $a \bmod m = b \bmod m = r$

there exist some integers s and t, s.t

$a = m \cdot s + r$, $b = m \cdot t + r$

$m \overline{)a}$ s r

$a - b = (ms + r) - (mt + r)$

$= ms + r - mt - r$

$a - b = m(s-t)$

by def of divisibility: $m \mid (a-b)$

by def of Modular Arithmetic $a \equiv b \pmod m$ ▨..

#18 Page 258

Ex. $a, b \in \mathbb{Z}$, $\underline{a \equiv 11 \pmod{19}}$ and $b \equiv 3 \pmod{19}$ Find the integer c with $\underline{0 \le c \le 18}$

s.t. a) $c \equiv 13a \pmod{19}$

way 1

way 2
by def
$19 \mid (a-11) \Rightarrow a-11 = 19\cdot k,\ k\in\mathbb{Z}$

$a \equiv 11 \pmod{19}$ theorem 3 : $a \bmod 19 = \underbrace{11 \bmod 19}$

$a \bmod 19 = 11$

$a = 19\cdot k + 11 \quad k\in\mathbb{Z}$

You can start from either one

way 1
$c \equiv 13a \pmod{19}$ by theorem 3. $c \bmod 19 = 13a \bmod 19$

$13a \bmod 19 \Rightarrow 13(19k+11) \bmod 19$

$= [\underbrace{\cancel{(13)\cdot(19k)}}_{0} + (13)(11)] \bmod 19$

$= (13)(11) \bmod 19$

$= 143 \bmod 19 \quad \Rightarrow 143 = 19\times 7 + 10$

$= 10$

$c \bmod 19 = 10 \qquad -9, 10, 29, 48, \ldots$

$c = 19\cdot k + 10$

$k=-2$,	$c=-28$
$k=-1$	, $c=-9$
$k=0$	, $c=10$
$k=1$	, $c=29$
$k=2$	, $c=48$
$k=3$	, $c=67$
	⋮

$c = 10$

e). $c \equiv \underbrace{2a^2+3b^2} \pmod{19}$

$a \equiv 11 \pmod{19} \Rightarrow a \bmod 19 = 11 \bmod 19 = 11 \Rightarrow a = 19k+11 \quad k\in\mathbb{Z}$

$b \equiv 3 \pmod{19} \Rightarrow b \bmod 19 = 3 \bmod 19 = 3 \Rightarrow b = 19\cdot t + 3 \quad t\in\mathbb{Z}$

$2a^2+3b^2 = 2(19k+11)^2 + 3(19t+3)^2$

$= 2\cdot[\cancel{(19k)^2} + \cancel{2(19k)(11)} + 11^2] + 3\cdot[\cancel{(19t)^2} + \cancel{2(19t)\cdot(3)} + 3^2]$

$(2a^2+3b^2) \bmod 19$

$= 2(121) + 3(9)$

$= 242 + 27 = \boxed{269}$

$c \equiv (2a^2+3b^2) \bmod 19$

$c \bmod 19 = (2a^2+3b^2) \bmod 19$

$= 269 \bmod 19 \Rightarrow 269 = 19\times 14 + 3$

$= 3$

$C \bmod 19 = 3$

$C = 19 \cdot S + 3$

$0 \le C \le 18$, $C = 3$

if $-18 \le C \le 18$, $\boxed{C = -16, 3}$

$S = -1 \Rightarrow C = -16$ × ↑

$S = 0 \Rightarrow C = 3$

$S = 1 \Rightarrow C = 22$ × ↓