Sect 8.3

(Ques: 4, 9, 30, 33, 43)

4/

$[a] = \{a\}$

$[b] = \{b, d\}$

$[c] = \{c\}$

$[d] = \{b, d\}$

9/ $A = \{\emptyset, \{-1\}, \{0\}, \{1\}, \{-1, 0\}, \{0, 1\}, \{-1, 1\}, \{-1, 0, 1\}\}$

$[\emptyset] = \{\emptyset\}$

$[-1] = \{-1, (-1, 0)\}$

$[0] = \{0, (-1, 1), (-1, 0, 1)\}$

$[1] = \{1, (0, 1)\}$

$[(-1, 0)] = \{-1, (-1, 0)\}$

$[(0, 1)] = \{1, (0, 1)\}$

$[(-1, 1)] = \{0, (-1, 1), (-1, 0, 1)\}$

$[(-1, 0, 1)] = \{0, (-1, 1), (-1, 0, 1)\}$

30/ Def: $(w, x)\ Q\ (y, z) \Leftrightarrow x = z$

a) Prove Q is equiv relation

_ Reflexive: $(w, x)\ Q\ (w, x)$ true since $x = x$

_ Symmetric: $(w, x)\ Q\ (y, z) \Rightarrow x = z$

Must show $(y, z)\ Q\ (w, x)$ true since $z = x$

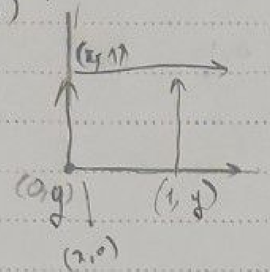
_ transitive: Let $(y, z)\ Q\ (a, b) \Leftrightarrow z = b$

Must show: $(w, x)\ Q\ (a, b)$ true since $x = z$ $\Big\} \rightarrow x = b$

b) $[(w, x)] = \{(w, x); (y, z)\}$

$[(y, z)] = \{(w, x); (y, z)\}$

33) It is a square



43)

a) Let $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$

$[(ad+bc, bd)] = [(a,b)] + [(c,d)] = [(a',b')] + [(c',d')] = [(a'd'+b'c', b'd')]$

b) Let $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$

$[(ac, bd)] = [(a,b)] \cdot [(c,d)] = [(a',b')][(c',d')] = [(a'c', b'd')]$

c) $[(a,b)] + [(0,1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)]$

$[(0,1)] + [(a,b)] = [(0 \cdot b + 1 \cdot a, 1 \cdot b)] = [(a,b)]$

$\Big\} [(a,b)] + [(0,1)] = [(0,1)] + [(a,b)] = [(a,b)]$

d) Find i,j so that $[(a,b)] \cdot [(i,j)] = [(ai, bj)] = [(a,b)]$

i,j so that $[(i,j)] \cdot [(a,b)] = [(ia, jb)] = [(a,b)]$

$\Big\} \Leftrightarrow i = 1, j = 1$

$(i,j) = (1,1)$

e) $[(-a,b)] + [(a,b)] = [(-ab + ba, b^2)] = [(0, b^2)]$

$[(a,b)] + [(-a,b)] = [(ab - ba, b^2)] = [(0, b^2)]$

f) Having ~~…~~ : $[(a,b)] \cdot [(c,d)] = [(c,d)] - [(a,b)] = [(1,1)]$

\- $[(a,b)] \cdot [(c,d)] = [(ac, bd)] = [(1,1)] \Leftrightarrow ac = 1 \wedge bd = 1$ (1)

\- $[(c,d)] - [(a,b)] = [(bc - ad, bd)] = [(1,1)] \Leftrightarrow bc - ad = 1 \wedge bd = 1$ (2)

(1), (2) $\Rightarrow$
$$\begin{cases} ac = 1 \rightarrow c = 1/a \\ bd = 1 \rightarrow d = 1/b \\ bc - ad = 1 \rightarrow \end{cases} \rightarrow (c,d) = \left(\frac{1}{a}, \frac{1}{b}\right)$$

Sect 8.4.

(Ques: 5, 11, 13, 37, 40)

5) Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

$\Leftrightarrow a = b + kn$ $\quad\Leftrightarrow b = c + ln$

for some $k, l \in \mathbb{Z}$

$a = b + kn = c + ln + kn = c + (l+k)n$

Therefor $a \equiv c \pmod{n}$

11) (base): $m = 1 \Leftrightarrow a \equiv c \pmod{n}$: True

(induct) Suppose $a^k \equiv c^k \pmod{n}$, $k \geq 1$

Must show that $a^{k+1} \equiv c^{k+1} \pmod{n}$

$a^{k+1} = a^k \cdot a$

$= (c^k + xn)(c + yn)$ for some $x, y \in \mathbb{Z}$

$= c^{k+1} + (cx + cy + xyn)n$

Let $cx + cy + xyn = l$

$\Rightarrow a^{k+1} = c^{k+1} + ln$

$\Leftrightarrow a^{k+1} \equiv c^{k+1} \pmod{n}$.

13)

a) (base): $n = 1$: $10^1 \equiv (-1) \pmod{11}$ True since $10 = -1 + 1 \cdot 11$

(induct) Suppose $10^k = (-1)^k \pmod{11}$

$10^{k+1} = 10^k \cdot 10$

$= [(-1)^k + 11n][-1 + 11]$

$= (-1)^{k+1} + 11(-1)^k - 11n + 11^2 n$

$= (-1)^{k+1} + 11[(-1)^k - n + 11n]$

Let $(-1)^k - n + 11n = x$.

$10^{k+1} = (-1)^{k+1} + x \cdot 11$

$\Leftrightarrow 10^{k+1} \equiv (-1)^{k+1} \pmod{11}$

b) Let a number abcd

Suppose $-a + b - c + d = 0 \pmod{11}$

$\Leftrightarrow a(-1) \pmod{11} + b \cdot 1 \pmod{11} + c(-1) \pmod{11} + d \cdot 1 \pmod{11} = 0 \pmod{11}$

$\Leftrightarrow a(-1)^3 \pmod{11} + b(-1)^2 \pmod{11} + c(-1)^1 \pmod{11} + d(-1)^0 \pmod{11} \equiv 0 \pmod{11}$

$\Leftrightarrow a \times 10^3 + b \times 10^2 + c \times 10^1 + d \times 10^0 \equiv 0 \pmod{11}$

$\Leftrightarrow \quad abcd \equiv 0 \pmod{11}$

$\Rightarrow \quad 11 \mid abcd$

37) $n = 713$; $p = 23$; $q = 31$, $e = 43$

encode : $C = 03$, $O = 15$, $M = 13$, $E = 05$

encrypt : $c = 3^{43} \bmod 713 = 675$

$o = 15^{43} \bmod 713 = 89$

$m = 13^{43} \bmod 713 = 476$ $\rightarrow$ convert to char?

$e = 5^{43} \bmod 713 = 129$

40) $\varphi(713) = 22 \cdot 30 = 660$

$ed \equiv 1 \pmod{660}$

$\Rightarrow d = 307$

- $028^{307} \pmod{713} = 14 \rightarrow N$
- $018^{307} \pmod{713} = 9 \rightarrow I$
- $675^{307} \pmod{713} = 3 \rightarrow C$
- $129^{307} \pmod{713} = 5 \rightarrow E$

Secr 9.1

(Ques: 4, 13, 19, 20)

4) Total number of card (sample space) : 52

Number of even-number card: $5 \times 4 = 20$ (card no. 2, 4, 6, 8, 10)

Number of even-number, black card : $20 : 2 = 10$

Event $= \frac{10}{52}$

13) a) Ques 1: C W

Ques 2: C W C W

Ques 3: C W C W C W C W

So, sample space : {CCC, CCW, CWC, CWW,

WCC, WCW, WWC, WWW} Size : Sample space = 8.

b) (i) CWW, WCW, WWC : 3

Probability $= \frac{3}{8}$

(ii) CCW, CWC, WCC (2 answers are correct): 3

CCC (3 answers are correct) : 1

$\Sigma = 4$

Probability $= 4/8 = \frac{1}{2}$

(iii) : WWW (0 answer is correct) = 1

Probability $= \frac{1}{8}$

19) 1^{st} ball : B_1 B_2

a) 2^{nd} ball : B_1 B_2 W_1 W_2 W_3 B_1 B_2 W_1 W_2 W_3

1^{st} ball W_1 W_2 W_3

2^{nd} ball: B_1 B_2 W_1 W_2 W_3 B_1 B_2 W_1 W_2 W_3 B_1 B_2 W_1 W_2 W_3

Size of sample space = 25

b) 1^{st} ball B_1 B_2

2^{nd} ball: B_1 B_2 W_1 W_2 W_3 B_1 B_2 W_1 W_2 W_3

Total outcomes = 10 Probability $= \frac{10}{25} = \frac{2}{5}$

c) 1st ball: W_1 W_2 W_3

2nd ball: W_1 W_2 W_3 W_1 W_2 W_3 W_1 W_2 W_3

Total outcomes $= 9$ Probability $= \frac{9}{25}$

20) Sample space's size $= 5$

Doors: A B C D E

Case 1: open B or C or D or E, win by A

Switch

Case 2: open B, $1/3$ win by C or D or E

Case 3: open C, $1/3$ win by B or D or E

Case 4: open D, $1/3$ win by B or C or E

Case 5: open E, $1/3$ win by B or C or D

a) Stick with door A, probability win $= 1/5$ $\left(= \frac{3}{15}\right)$

b) Switch probability win $= \underbrace{\left(\frac{1}{5} \times \frac{1}{3}\right)}_{\text{Case 2}} + \underbrace{\left(\frac{1}{5} \times \frac{1}{3}\right)}_{\text{Case 3}} + \underbrace{\left(\frac{1}{5} \times \frac{1}{3}\right)}_{\text{Case 4}} + \underbrace{\left(\frac{1}{5} \times \frac{1}{3}\right)}_{\text{Case 5}} = \frac{4}{15}$

Sect 11.5

(Ques: 4, 18, 25, 26)

4) Let $\frac{n^2}{10} = n\log_2 n$

when $n > 1.078$, $\frac{n^2}{10}$ is better ; $1 < n \leq 1.078$, $n\log_2 n$ is better.

From $0 < n < 1$, can use $n^2/10$ only.

18) Let $a[end] = k$, $a[start] = 1$, so length of array is $k - 1 + 1 = k$

Suppose input $x \neq a[mid]$, know that $a[mid] = k/2$

Case 1: k even

if $x < a[mid]$, $a[end] = \frac{k}{2} - 1$, then length of array is $\left(\frac{k}{2} - 1\right) - 1 + 1 = \frac{k}{2} - 1 < \frac{k}{2}$

Similar to $x > a[mid]$, array's length is $\frac{k}{2} - 1$

Case 2: k odd

If $x < a[mid]$, $a[end] = \frac{k}{2}$, then length of array is $\frac{k}{2} - 1 + 1 = \frac{k}{2}$

Similar to $x > a[mid]$

So, array's length after 1 iteration is $\leq \frac{k}{2}$

25)

a) (Base): $n = 1$: $m_1 = 0$; $\frac{1}{2} \cdot 1 \cdot \log_2 1 = 0$ True

(Induct): Suppose $\frac{1}{2} k \log_2 k \leq m_k$ holds for k st. $1 \leq k \leq n$

Must show that it holds for $n+1$.

Note: $m_{n+1} = m_{\lfloor \frac{n+1}{2} \rfloor} + m_{\lceil \frac{n+1}{2} \rceil} + n + 2$

Case 1: $n+1$ is even

$m_{n+1} = 2\, m_{\frac{n+1}{2}} + n + 2 \geq \left(\frac{n+1}{2}\right) \log_2\left(\frac{n+1}{2}\right) + n + 2$ $\quad\left(\frac{n+1}{2} \leq n \text{ for } n \geq 1\right)$

$\Leftrightarrow m_{n+1} \geq \frac{1}{2}(n+1)\log_2(n+1) - \frac{n}{2} + n - \frac{1}{2} + 2 \geq \frac{1}{2}(n+1)\log_2(n+1)$ $\quad\left(\text{since } \frac{n}{2} + \frac{3}{2} > 0\right)$

Case 2: $n+1$ is odd

$m_{n+1} = m_{\frac{n}{2}} + m_{\frac{n+2}{2}} + n + 2 \geq \frac{1}{2}\left(\frac{n}{2}\right)\log_2 \frac{n}{2} + \frac{1}{2}\left(\frac{n+2}{2}\right)\log_2 \frac{n+2}{2} + n + 2$ (1)

Since $\frac{n+2}{2} \leq n$ for $n \geq 2$, but there exists only m_3, m_5, for $n+1$ odd, so induct. hypo holds

(1) $\Leftrightarrow m_{n+1} \geq \frac{1}{2}\left(\frac{n}{2}\right)\log_2 n + \frac{1}{2}\left(\frac{n+1}{2}\right)\log_2(n+1) + \frac{n}{2} + \frac{3}{2} \geq \frac{1}{2}(n+1)\log_2(n+1)$

b/ (base) $n=1$: $m_1 = 0$, $2 \cdot 1 \cdot \log_2 1 = 0$ True

(induc) Suppose $m_k \leq 2k\log_2 k$ true for $1 \leq k \leq n$

$m_{n+1} = m_{\lfloor \frac{n+1}{2} \rfloor} + m_{\lceil \frac{n+1}{2} \rceil} + n+2$

Case 1: $n+1$: even : $m_{n+1} = 2\, m_{\frac{n+1}{2}} + n+2 \leq 2\left[2\left(\frac{n+1}{2}\right)\log\left(\frac{n+1}{2}\right)\right] + n+2 = 2(n+1)\log_2(n+1) - n$

$\leq 2(n+1)\log_2(n+1)$

Case 2: $n+1$: odd : $m_{n+1} \leq 2\left(\frac{n}{2}\right)\log_2\left(\frac{n}{2}\right) + 2\left(\frac{n+2}{2}\right)\log_2\left(\frac{n+2}{2}\right) + n+2$

$= n\log_2 n - n + (n+2)\log_2(n+2) - n - 2 + n + 2$

$= n\log_2 n + (n+2)\log_2(n+2) - n \leq 2(n+1)\log_2(n+1)$

26)

a) (i) input n ; array[ ] , $i = 0$; number : x st x^n

while ($n \geq 1$) :

array[i] = n % 2

i ++

n = n/2

The array[ ] contains $\{k, k-1, k-2, \dots, \}$ st $k \cdot 2^0$, $(k-1)2^1$,

knowing $k, k-1$ are 1 or 0.

ii) Array value X[ ] st $\{x^{k \cdot 2^0}, x^{(k-1)2^1}, \dots\}$

for j in range i :

num = array[j] $\cdot\ 2^i$

value X[j] = x^{num}

iii) result = 1

for j in range i

result *= value X[j]

b) Multiplications in (ii) : $\lfloor \log_2 n \rfloor$

Multiplications in (iii) : $\lfloor \log_2 n \rfloor - k$

$\Big\}\ 2\lfloor \log_2 n \rfloor - k \leq 2\lfloor \log_2 n \rfloor$

Note : $k = 1$ if set result = value X[0]

$k = 0$ if set result = 1