4.3

2 $n=0$ $a_0: \frac{0^2}{2(0)-1} = 0$

$n=1$ $a_1: \frac{(1)^2}{2(1)-1} = 1$

$n=2$ $a_2: \frac{2^2}{2(2)-1} = 4/3$

$n=3$ $a_3: \frac{3^2}{2(3)-1} = 9/5$

6 a. $a_n = (-1)^{n+1}$

b. $a_n = \begin{cases} 0, & \text{when } n \text{ is odd} \\ 2, & \text{when } n \text{ is even} \end{cases}$

c. $a_n = 2n-1$

d. $a_n = 2(n^2)$

e. $a_n = 2n!$

f. $a_n = 2(3^n)$

g $a_n = 3n-2$

h $a_n = 4n-7$

i $a_n = n^2 - 2 \cdot n + 2$

j $a_n = 5$

8 1. $a_n = 3^{n-1}$ 2. $a_n = \frac{n^2-n+3}{3}$ 3. $a_n = 4^{n-1} - n! + 1$

10 a. $X_1 = 10010$ $X_2 = 01011$ $X_3 = 00101$

b. $S_1 = \emptyset$ $S_2 = \{X_2, X_5\}$ $S_3 = \{X_1, X_2, X_3, X_4, X_5\}$

12 $A_2 = \{2\}$ $A_3 = \{3\}$ $A_4 = \{2, 4\}$ $A_5 = \{1, 2, 3, 5\}$

$A_6 = \{1, 2, 3, 4, 6\}$

5.1

2 $A \times B = \{(w,x), (w,y), (w,z), (x,y), (x,x), (x,z), (y,x), (y,y), (y,z)\}$

a.

b $R = \{(w,x), (w,y), (w,z), (x,y)\}$

c. $R = \{(w,x), (w,y), (w,w), (x,y), (x,x)\}$

4 A to B $= \{(1,3), (1,5), (2,3), (2,4), (2,5), (3,7), (3,5)\}$

8 Consider a nonempty set S such that $R = S \times S$
This in turn satisfies all properties

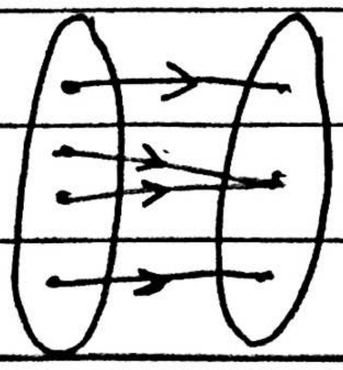
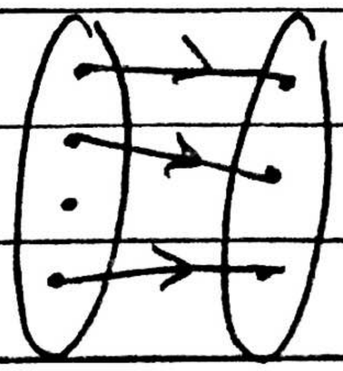
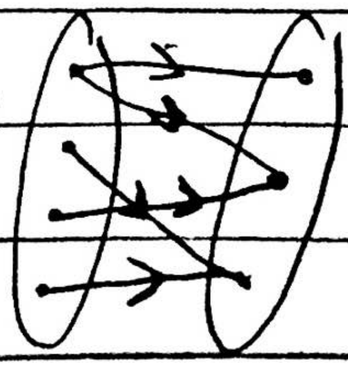
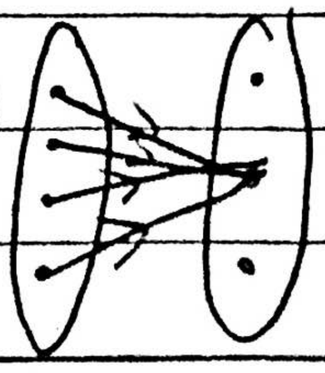
5.2

2 $[1] = \{x \in S \mid xR1\} = \{1,3,4\}$
$[2] = \{x \in S \mid xR2\} = \{2\}$
Also $[5] = \{x \in S \mid xR5\} = \{5,7\}$
$[6] = \{x \in S \mid xR6\} = \{6\}$

$[1] = \{1,3,4\}$
$[2] = \{2\}$
$[5] = \{5,7\}$
$[6] = \{6\}$

4 $R = \{(x,x), (x,y), (x,u), (y,x), (u,x), (y,y), (u,u), (v,v), (v,z), (z,v), (z,z), (w,v)\}$

5.3

2 f_1  f_2  f_3  f_4 

4 There is some element $x \in X$ such that it is not a unique pre image point

8 $g = \{(1,x), (2,y), (3,z), (4,x)\}$
$h = \{(x,1), (y,2), (z,3)\}$

10 $f_1 = \{(a,0),(b,0),(c,0)\}$ $f_2 = \{(a,0),(b,0),(c,1)\}$
$f_3 = \{(a,0),(b,1),(c,0)\}$ $f_4 = \{(a,0),(b,1),(c,1)\}$
$f_5 = \{(a,1),(b,0),(c,0)\}$ $f_6 = \{(a,1),(b,0),(c,1)\}$
$f_7 = \{(a,1),(b,1),(c,1)\}$ $f_8 = \{(a,1),(b,1),(c,1)\}$

12 $S = \{-2,-1,0,1,2\}$
$r = \{(x,y) \in S \times S : |x| + |y| = 2\}$
$= \{(-2,0),(-1,-1),(-1,1),(0,2),(1,1),(1,-1),(2,0)\}$
Since -1 has two image points therefore f is not a function

16 $I_1 = \{(t,t),(u,u),(v,v)\}$
$I_2 = \{(\emptyset,\emptyset),(\{1\},\{1\}),(\{2\},\{2\}),(\{1,2\},\{1,2\})\}$

18 a. 1, 0, 0, -1 b. 2, -1, 2, -2 c. 3, -3, 3, -3

20 a. $f(S) = \{2\}$ b. $f(S) = \{-3,-1,1,3,5\}$
c. $f(S) = \{1,2,5\}$ d. $f(S) = \{1,3,5\}$ e. $f(S) = \{0,1\}$

26 a. Range $f = \{0\}$ b. Range $f = \mathbb{Z}$ c. Range $f = \mathbb{R}$
d. Range $f = \mathbb{Q}$ e. Range $= \{1,2,3,4,\ldots,9\}$

28 a. $(g \circ f)(1) = 4$, $(g \circ f)(2) = 1$, $(g \circ f)(3) = 3$
b. $g \circ f = \{(1,4),(2,1),(3,3)\}$

30 a. $(g \circ f)(1) = 1$, $(f \circ g)(b) = c$
b $(g \circ f)(3) = g(f(3))$, $(g \circ f)(4) = g(f(4))$
$= g(c)$ $= g(d)$
$= 2$ $= 1$
$g \circ f = \{(1,1),(2,1),(3,2),(4,1)\}$
$f \circ g = \{(a,a),(b,c),(c,a),(d,a)\}$

32 a. $(g \circ f)(-4) = 2$

b. $(f \circ g)(5) = 3$

5.4

2 a. $f(n) = f(m)$ $f(n) = 4n+1 : n \in \mathbb{Z}$

$\Rightarrow 4n+1 = 4m+1 = 4n = 4m = n = m$

Which implies $f: A \to B$ is one to one

b. $f(x) = x^2 : x \in \mathbb{R}^+$

$\Rightarrow f(x) = f(y)$

$\Rightarrow x^2 = y^2 = \sqrt{x^2} = y^2 = x = y$ Checks out

c. $f(x) = \lceil x \rceil : x \in \mathbb{R}$

$\Rightarrow f(x) = f(y) \Rightarrow \lceil x \rceil = \lceil y \rceil$

$x = 0.3$ & $y = 0.6 \Rightarrow \lceil 0.3 \rceil = \lceil 0.6 \rceil$

$= 0 = 0$

2 elements of the domain cannot map to the same element in the range

not one to one

d. $f(x) = x^2 + 2x + 1 : x \in \mathbb{R}$

$\Rightarrow f(x) = x^2 + 2x + 1 = (x+1)^2$

$f(x) = f(y) \Rightarrow (x+1)^2 = (y+1)^2$ let $x = 6$ & $y = -8$

$= (6+1)^2 = (-8+1)^2$

$= 49 = 49$

Not one to one

4 $f(x) = 2x+1 : x \in \mathbb{R}$, $y = f(x)$

$y = 2x+1$

$y-1 = 2x$

$(y-1)/2 = x \in \mathbb{R}$

$f(x) = 2x+1$

$f\left(\frac{y-1}{2}\right) = 2\left(\frac{y-1}{2}\right)+1 = f\left(\frac{y-1}{2}\right) = y-1+1 = f\left(\frac{y-1}{2}\right) = y$

6 a. Each element of $f_2 + f_3$ in range have unique domain $\Rightarrow$ $f_2 + f_3$ are one to one.

In f_1 2nd + 3rd element map at same element so f_1 is not one to one + f_4 has 1, 2, + 4 element map to the same range

- One to One: $f_2 + f_3$ Not: $f_1 + f_4$

b. $f_1 + f_3$ are onto, $f_2 + f_4$ are not onto

8 $|A| = 4$ + $|B| = 3$ since $|A| \geq |B|$

This implies that there does not exist any one to one

10 • $A = \{a, b, c, d\}$ + $B = \{q, r, s, t, u\}$

$f: A \to B$

$f(a) = q$

$f(b) = r$

$f(c) = s$

$f(d) = t$

Since every element in the D maps to some unique R, + One R has no D f is one to one + not onto

• $g: B \to A$, $g(q) = a$, $g(r) = b$, $g(s) = c$, $g(t) = d$, $g(u) = a$

- 2 elements in D map to 1 R so not one to one
- each R has a preimage in D

12 a. $f(n) = n-5$, $f(n) = f(m) \Rightarrow n-5 = m-5$

$\Rightarrow n = m$

f is one to one

b $y \in \mathbb{Z}$, $x = y+5 \in \mathbb{Z}$

$f(x) = f(y+5)$

$= y+5-5 = y$ hence onto

14 a. i. $f(n) = f(m) \Rightarrow 3n+5 = 3m+5$

$n = m$ = one to one

ii. $y = 7 \in \mathbb{Z}$ such that no clear $x \in \mathbb{Z}$ exists

So not onto

b. i. $g(n) = g(m) \Rightarrow 3n+5 = 3m+5$

$n = m$ = one to one

ii. $g(x) = 3x+5$ clearly a $y \in \mathbb{R}$ exists

$x = \frac{y-5}{3} \in \mathbb{R}$ so yes onto

16 a. $f(x) = f(y) \Rightarrow 5x-1 = 5y-1 \Rightarrow x = y$ so one to one

$\Rightarrow y = f(x) = y = 5x-1$

$y+1 = 5x = \frac{y+1}{5} = x$ so onto

hence proved bijective

b. $f(x) = f(y) = x^2+x+1 = y^2+y+1$ :: let $x=0$ & $y=-1$

$0+1 = 1-1+1 \Rightarrow 1=1$

not one to one

∴ not bijective

c. $f(x)=f(y) \Rightarrow 2x^3+3=2y^3+3$

$y^3=y^3 = x=y$ so 1 to 1

$y=f(x) \Rightarrow y=2x^3+3$

$y-3=2x^3$

$\frac{y-3}{2}=x^3 = \left(\frac{y-3}{2}\right)^{1/3}=x$ ∴ on to

∴ not bijective

d. $f(x)=f(y) \rightarrow x^4+3x^2+1=y^4+3y^2+1$ $x=0.5, y=-0.5$

$(0.5)^4+3(0.5)^2+1=(-0.5)^4+3(-0.5)^2+1$

$1.\delta = 1.\delta$ ∴ not one to one

0 has no pre image in D ∴ not bijective

28 f: A→A is not bijective

Since 1 element of the R has no preimage in D

⇒ f: A→A is not onto

Theorem states a function f: A→B has an inverse

iff f is bijective

⇒ not bijective, no inverse

30 $f^{-1}(u)=p$, $f^{-1}(w)=q$, $f^{-1}(t)=r$, $f^{-1}(v)=s$

32 $f(n)=f(m) \Rightarrow 2-n^3=2-m^3$, $n=m$ is one to one

$x=\sqrt[3]{(2-y)}$ ∴ f is onto

$f^{-1}(x)=\sqrt[3]{(2-x)}$ for $x \in \mathbb{R}$

7.1

2 a. 6, 9, 15

$6=3\times(a)$, $a=2$

$9=3\times(a)$, $a=3$

$15=3\times(a)$, $a=5$

b. 10, 15, 25 $10 = 5a \quad a = 2$

$15 = 5a \quad a = 3$

$25 = 5a \quad a = 5$

c. 30 $2 \cdot 5 \cdot 3 = 30$

d. 12

e. 24

f. 12

4 $b = ax + a \mid (b + c)$

$b + c = ay \Rightarrow ax + c = ay$

$\Rightarrow c = ay - ax$

$= a(y - x)$

Since $y - x$ is an integer

$\therefore a \mid c$

6 $a \mid b \quad \therefore b = ax \Rightarrow |x| \geq 1$

$|b| = |ax|$

$= |a||x|$

$\geq |a| \cdot 1$

$= |a| \Rightarrow |a| \leq |b|$

8 $3 \mid b, \quad b = 3x, \quad a = 3y$

$a + b = 3y + 3x$

$= 3(y + x) \Rightarrow 3$ divides $a + b$ this contradicts the hypothesis

10 a. $n = 36x$

$= 12(3x) \Rightarrow n$ is a multiple of 12

b. $12 \mid 36 + 36 \mid n \therefore 12 \mid n$

$\Rightarrow n$ is a multiple of 12

12 $P(n): 3 \mid (2^{2n}-1)$

$n=0$, since $3 \mid 0$ thus $P(n)$ is true for $n=0$

$n=k+1 \quad 3 \mid (2^{2(k+1)}-1)$

$2^{2(k+1)}-1 = 2^{2k}\cdot 2^2 - 1$

$= 2^{2k}\cdot 2^2 - 2^2 + 2^2 - 1$

$= 2^2(2^{2k}-1) + 3$

$= 4(3x) + 3$

$\Rightarrow 2^{2(k+1)}-1 = 3(4x)+3$

$= 3(4x+1)$ ∈ ℤ ✓ true for $k+1$

So true

14 $P(n): 4 \mid (7^n - 3^n)$, $n=0$

$4 \mid 0$ is true

$4 \mid 7^{k+1} - 3^{k+1}$

$7^{k+1} - 3^{k+1} = 7^{k+1} - 7^k\cdot 3 + 7^k\cdot 3 - 3^{k+1}$

$= 7^k(7-3) + 3(7^k - 3^k)$

$= 7^k\cdot 4 + 3(4x)$

$= 4(7^k + 3x)$

$\Rightarrow 4 \mid 7^{k+1} - 3^{k+1}$ thus true

so true

7.2

2 a. 127 is prime b. 129 is not prime

c. 131 is prime d. 133 is prime

7.3

16 $3 \nmid a^2 \Rightarrow a^2 = 3k+1$ or $a^2 = 3k+2$

$a^2 - 1 = 3k \Rightarrow a^2 - 1$ is divisible by 3

hence proven

18 $3 \mid n \Rightarrow n = 3k : k \in \mathbb{Z}$

$2n^2 + 1 = 2(3k)^2 + 1$

$= 18k^2 + 1$ hence proven

7.4

2 a. true b. true c. true d. true

4 a. $a = 40, b = 5, n = 7$

$a - b = 40 - 5$

$= 35$ $n \mid (a-b)$ as $7 \mid 35$

$\therefore$ 40 is congruent to 5 mod 7

b. $a = 108, b = 5, n = 7$

$a - b = 108 - 5 = 103$, $n \nmid (a-b)$ as $7 \nmid 103$

hence not congruent

c. $a = -29, b = 5, n = 7$

$a - b = -29 - 5 = -34$

$\therefore$ not congruent

d. $a = -122, b = 5, n = 7$

$a - b = -122 - 5 = -127$

$\therefore$ not congruent

6

6 $a, b, + n \geq 2$ $a \equiv b \pmod n$ iff $a = b + kn$

$a \equiv b \pmod n$

$b \equiv c \pmod n$, $b = c + ln$

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

for some $p = k + l$, $a = c + pn$

so, $a \equiv c \pmod n$

10 $a \equiv (\mod n) b$ iff $a = b + kn$ for some k

so $a = b + kn$

$c \equiv d \pmod n$

so $c = d + ln$

$ac = (b+kn)(d+ln)$

$= b(d+ln) + kn(d+ln)$

$= bd + bln + knd + knln$

$= bd + (bl + kd + knl)n$ for some $p = bl + kd + knl$

$ac = bd + pn$

7.5

2 SOS RADARN

4 HIGH OPPS

7.5 RSA

1. Bobs Public Key
2. Yes, its prime
3. No, 187 not divisible by 5

4 RSA mod $n = 55$, $e = 3$