1\. a. The <u>contrapositive</u> of $P \Rightarrow Q$ is $(\text{NOT } Q) \Rightarrow (\text{NOT } P)$

P	Q	$P \Rightarrow Q$	NOT Q	NOT P	$(\text{NOT } Q) \Rightarrow (\text{NOT } P)$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The truth tables for $P \Rightarrow Q$ and $(\text{NOT } Q) \Rightarrow (\text{NOT } P)$ are the same, so they are logically equivalent

b. The <u>converse</u> of $P \Rightarrow Q$ is $Q \Rightarrow P$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

The truth tables for $P \Rightarrow Q$ and $Q \Rightarrow P$ are different, so they are <u>not</u> logically equivalent.

2 a. $A \cup B = \{x \mid (x \in A) \text{ OR } (x \in B)\}$

$A \cap B = \{x \mid (x \in A) \text{ AND } (x \in B)\}$

$A \setminus B = \{x \mid (x \in A) \text{ AND } (x \notin B)\}$

b. Let $P = (x \in A)$, $Q = (x \in B)$, $R = (x \in C)$

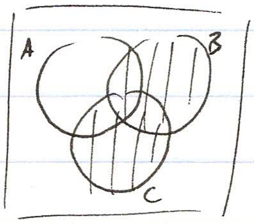
Then

$$\left.\begin{aligned} (x \in A \cap (B \cup C)) &= P \text{ AND } (Q \text{ OR } R) \\ (x \in (A \cap B) \cup (A \cap C)) &= (P \text{ AND } Q) \text{ OR } (P \text{ AND } R) \end{aligned}\right\} (*)$$

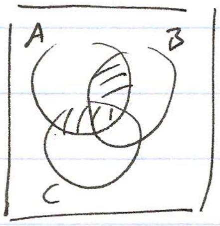
P	Q	R	Q OR R	P AND (Q OR R)	P AND Q	P AND R	(P AND Q) OR (P AND R)
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

The truth tables for P AND (Q OR R) and (P AND Q) OR (P AND R) are the same, so they are logically equivalent. So by $(*)$ we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Alternatively, using Venn diagrams:-

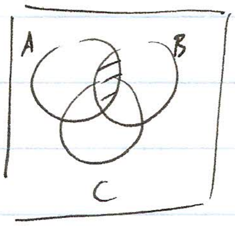


$B \cup C$

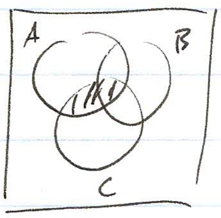


$A \cap (B \cup C)$

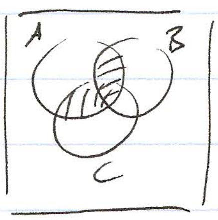
We see that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



$A \cap B$



$A \cap C$



$(A \cap B) \cup (A \cap C)$

c. Let $P = (x \in A)$, $Q = (x \in B)$, $R = (x \in C)$

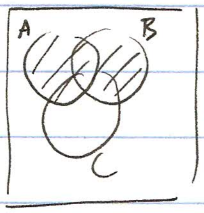
Then $(x \in (A \cup B) \setminus C) = (P \text{ OR } Q) \text{ AND } (\text{NOT } R)$

$(x \in (A \setminus C) \cup (B \setminus C)) = (P \text{ AND } (\text{NOT } R)) \text{ OR } (Q \text{ AND } (\text{NOT } R))$ $\Big\}$ $(*)$

P	Q	R	P OR Q	NOT R	(P OR Q) AND (NOT R)	P AND (NOT R)	Q AND (NOT R)	(P AND (NOT R)) OR (Q AND (NOT R))
T	T	T	T	F	F	F	F	F
T	T	F	T	T	T	T	T	T
T	F	T	T	F	F	F	F	F
T	F	F	T	T	T	T	F	T
F	T	T	T	F	F	F	F	F
F	T	F	T	T	T	F	T	T
F	F	T	F	F	F	F	F	F
F	F	F	F	T	F	F	F	F

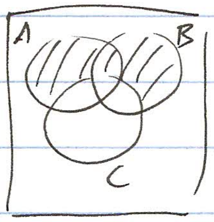
The truth tables for $(P \text{ OR } Q) \text{ AND } (\text{NOT } R)$ and $(P \text{ AND } (\text{NOT } R)) \text{ OR } (Q \text{ AND } (\text{NOT } R))$ are the same, so they are logically equivalent. So by $(*)$, we have $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$

Alternatively, using Venn diagrams:-



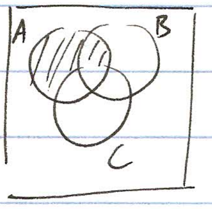
$A \cup B$

$\rightsquigarrow$



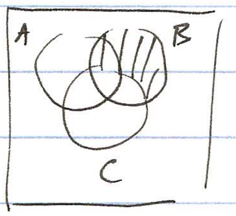
$(A \cup B) \setminus C$

We see that $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$



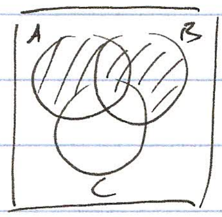
$A \setminus C$

,



$B \setminus C$

$\rightsquigarrow$



$(A \setminus C) \cup (B \setminus C)$

3. a. For all positive integers x, $x \geq 1$
b. For all real numbers x, $x^2 \geq 0$.
c. There is a real number x such that $x^2 - 6x + 7 = 0$.
d. There is an integer x such that $x^2 \equiv 2 \bmod 7$.
e. For all real numbers x and y, if $xy = 0$ then $x = 0$ or $y = 0$.
f. For all positive integers x there exists a positive integer y such that $y > x$.
g. For all real numbers y there is a real number x such that $x^3 = y$.

logically equivalent

4. a. $\text{NOT}\left((\exists x \in \mathbb{Z})(x^2 \equiv 3 \bmod 4)\right) \equiv (\forall x \in \mathbb{Z})(x^2 \not\equiv 3 \bmod 4)$

For all integers x, $x^2 \not\equiv 3 \bmod 4$.

b. $\text{NOT}\left((\forall x \in \mathbb{R})(x^2 - 4x + 2 > 0)\right) \equiv (\exists x \in \mathbb{R})(x^2 - 4x + 2 \leq 0)$

~~For all real number~~ There is a real number x such that $x^2 - 4x + 2 \leq 0$.

c. $\text{NOT}\left((\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(y < x)\right) \equiv (\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(y \geq x)$

There is a positive integer x such that for all positive integers y, $y \geq x$.

d. $\text{NOT}\left((\exists b \in \mathbb{R})(\forall x \in \mathbb{R})(\log x \leq b)\right) \equiv (\forall b \in \mathbb{R})(\exists x \in \mathbb{R})(\log x > b)$

For all real numbers b there is a real number x such that $\log x > b$.

e NOT $((\exists x,y,z \in \mathbb{N})(x^3+y^3=z^3)) \equiv (\forall x,y,z \in \mathbb{N})(x^3+y^3 \neq z^3)$

For all positive integers $x, y, \& z$, $x^3+y^3 \neq z^3$.

5 a. $(\forall x \in \mathbb{R})(x^2+2x+3>0)$

b. $(\exists x \in \mathbb{R})(x^2=2)$

c. $(\forall n \in \mathbb{N})(\exists a \in \mathbb{R})((x \geq a) \Rightarrow (e^x \geq x^n))$

d. $(\exists b \in \mathbb{R})(\forall x \in \mathbb{R})(x - x^2 \leq b)$

6. $a_1 = 10$, $a_{n+1} = 3a_n - 8$ for $n \in \mathbb{N}$

Claim: $a_n = 2 \cdot 3^n + 4$ for all $n \in \mathbb{N}$

Proof: By induction.

$n=1$ $a_1 = 10$ and $2 \cdot 3^1 + 4 = 6 + 4 = 10$ ✓

$n=k \Rightarrow n=k+1$. We assume $a_k = 2 \cdot 3^k + 4$ and show that

$a_{k+1} = 2 \cdot 3^{k+1} + 4$:—

$$a_{k+1} = 3a_k - 8 = 3(2 \cdot 3^k + 4) - 8 = 2 \cdot 3 \cdot 3^k + 12 - 8$$
$$= 2 \cdot 3^{k+1} + 4. \quad \square$$

7. Claim $\sum_{r=1}^{n} (2r+1) = n(n+2)$ for all $n \in \mathbb{N}$.

Proof: By induction

$n=1$ LHS $= (2 \cdot 1 + 1) = 3$. RHS $= 1 \cdot (1+2) = 3$ ✓

$n=k \Rightarrow n=k+1$: We assume $\sum_{r=1}^{k} (2r+1) = k(k+2)$ and show that

$\sum_{r=1}^{k+1} (2r+1) = (k+1)((k+1)+2)$.

$$\text{LHS} = \sum_{r=1}^{k} (2r+1) + (2(k+1)+1) = k(k+2) + (2k+3) = k^2+2k+2k+3$$
$$= k^2+4k+3$$

RHS $= (k+1)(k+3) = k^2+4k+3$ ✓. $\square$

8. <u>Claim</u> $\displaystyle\sum_{r=1}^{n} r(r+2) = \frac{1}{6} n(n+1)(2n+7)$ for all $n \in \mathbb{N}$.

<u>Proof</u>. By induction

<u>$n=1$</u> LHS $= 1\cdot(1+2) = 3$. RHS $= \frac{1}{6}\, 1\cdot(1+1)(2\cdot 1+7) = \frac{1}{6}1\cdot 2\cdot 9 = 3$. ✓

<u>$n=k \Rightarrow n=k+1$</u>: We assume $\displaystyle\sum_{r=1}^{k} r(r+2) = \frac{1}{6} k(k+1)(2k+7)$

and show $\displaystyle\sum_{r=1}^{k+1} r(r+2) = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+7)$

$$\text{LHS} = \sum_{r=1}^{k} r(r+2) + (k+1)((k+1)+2) = \frac{1}{6} k(k+1)(2k+7) + (k+1)(k+3)$$

$$= \frac{1}{6}(k+1)(k(2k+7) + 6(k+3))$$

$$= \frac{1}{6}(k+1)(2k^2+13k+18)$$

$$\text{RHS} = \frac{1}{6}(k+1)(k+2)(2k+9) = \frac{1}{6}(k+1)(2k^2+13k+18) \checkmark$$

$\square$.

9. <u>Claim</u> $5^n > 4^n + 3^n + 2^n$ for all $n \in \mathbb{N}$ such that $n \geq 3$.

<u>Proof</u> By induction.

<u>$n=3$</u> $5^3 = 125$, $4^3+3^3+2^3 = 64+27+8 = 99$,

$125 > 99$ ✓.

<u>$n=k \Rightarrow n=k+1$</u>. We assume $5^k > 4^k+3^k+2^k$ and show

$5^{k+1} > 4^{k+1}+3^{k+1}+2^{k+1}$

$$5^{k+1} = 5\cdot 5^k > 5\cdot(4^k+3^k+2^k) = 5\cdot 4^k + 5\cdot 3^k + 5\cdot 2^k$$
$$> 4\cdot 4^k + 3\cdot 3^k + 2\cdot 2^k$$
$$= 4^{k+1}+3^{k+1}+2^{k+1}.$$

$\square$.

10 a. 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

b. Claim $f_1^2 + f_2^2 + \dots + f_n^2 = f_n \cdot f_{n+1}$ for all $n \in \mathbb{N}$.

Proof. By induction.

$n=1$. LHS $= f_1^2 = 1^2 = 1$

RHS $= f_1 \cdot f_2 = 1 \cdot 1 = 1$ ✓

$n=k \Rightarrow n=k+1$. We assume $f_1^2 + \dots + f_k^2 = f_k \cdot f_{k+1}$

and show $f_1^2 + \dots + f_{k+1}^2 = f_{k+1} f_{(k+1)+1}$:-

$$\text{LHS} = f_1^2 + \dots + f_k^2 + f_{k+1}^2 = (f_1^2 + \dots + f_k^2) + f_{k+1}^2$$
$$= (f_k \cdot f_{k+1}) + f_{k+1}^2 = f_{k+1} \cdot (f_k + f_{k+1})$$
$$= f_{k+1} \cdot f_{k+2} = \text{RHS}$$

by definition of Fibonacci sequence

$\square$.

11 a. The greatest common divisor of a & b is the largest $d \in \mathbb{N}$ such that $d | a$ and $d | b$.

$\gcd(123, 39) = ?$

Use Euclidean algorithm

$123 = 3 \cdot 39 + 6$

$39 = 6 \cdot 6 + \boxed{3}$

$6 = 2 \cdot 3 + 0$

$\gcd(123, 39) = 3.$

b. $\gcd(157, 83) = ?$

$157 = 1 \cdot 83 + 74$

$83 = 1 \cdot 74 + 9$

$74 = 8 \cdot 9 + 2$

$9 = 4 \cdot 2 + \boxed{1}$

$2 = 2 \cdot 1 + 0.$

$\gcd(157, 83) = 1.$

c $\gcd(2^5 3^7 5^9 11^4, 2\cdot 3^2 7^{10}) = 2\cdot 3^2 = 12.$

using $\gcd(p_1^{\alpha_1}\cdots p_r^{\alpha_r}, p_1^{\beta_1}\cdots p_r^{\beta_r}) = p_1^{\min(\alpha_1,\beta_1)}\cdots p_r^{\min(\alpha_r,\beta_r)}$

for $p_1,\dots,p_r$ primes and $\alpha_1,\dots,\alpha_r,\beta_1,\dots,\beta_r \in \mathbb{Z}_{\geq 0}$.
(follows from the fundamental theorem of arithmetic.)

12. Claim $\gcd(3n+2, 3n+5) = 1$ for all $n \in \mathbb{N}$.

Proof. By Euclidean algorithm:-

$$\begin{aligned} 3n+5 &= 1\cdot(3n+2) + 3 \\ 3n+2 &= n\cdot 3 + 2 \\ 3 &= 1\cdot 2 + \boxed{1} \\ 2 &= 2\cdot 1 + 0 \end{aligned}$$

$\gcd(3n+5, 3n+2) = 1.$ ∎

13. a. $24x + 52y = 8$

$\gcd(24, 52) = 4 \mid 8 \implies$ solutions exist.

EA: $52 = 2\cdot 24 + \boxed{4}$, $24 = 6\cdot 4 + 0$.

$4 = 24\cdot(-2) + 52\cdot(1)$ (solve $ax+by=\gcd(a,b)$ using back subst. in EA)

$\times 2$ $8 = 24\cdot(-4) + 52\cdot(2) \implies$ one solution is $x=-4, y=2$.

All solutions of $ax+by=c$ are given by $x = x_0 + \frac{b}{d}\cdot t$, $y = y_0 - \frac{a}{d}\cdot t$,
where x_0, y_0 is one solution and $d = \gcd(a,b)$. for $t\in\mathbb{Z}$ arbitrary.

In our case: $x = -4 + \frac{52}{4}t$, $y = 2 - \frac{24}{4}t$

$= -4 + 13t$ $= 2 - 6t$

b. $\gcd(42, 15) = 3 \nmid 7 \implies$ no solutions.

14. a) $5x \equiv 12 \mod 17$

$\iff 5x = 17q + 12$, some $q \in \mathbb{Z}$

$\iff 5x + 17y = 12$ $\quad y = -q$

One solution : $x = -1,\ y = 1$ (By inspection, or use EA)

All solutions $x = -1 + 17t,\ y = 1 - 5t$ $(\gcd(5,17) = 1)$

$\therefore$ $5x \equiv 12 \mod 17 \iff x \equiv -1 \mod 17$.

b) $x^2 + 3x + 1 \equiv 0 \mod 5$

Cases $x \equiv 0, 1, 2, 3$ or $4 \mod 5$

x	0	1	2	3	4
x^2+3x+1	1	$5 \equiv 0$	$11 \equiv 1$	$19 \equiv 4$	$29 \equiv 4$

So $x^2 + 3x + 1 \equiv 0 \mod 5 \iff x \equiv 1 \mod 5$.

15 a) $x^3 + x + 1 \equiv 0 \mod 4$.

Cases $x \equiv 0, 1, 2,$ or $3 \mod 4$

x	0	1	2	3
x^3+x+1	1	3	$11 \equiv 3$	$31 \equiv 3$

So there are <u>no solutions</u> of $x^3 + x + 1 \equiv 0 \mod 4$.

b) <u>Claim</u>: The equation $x^3 + x = 4y^2 + 7$ has no solutions $x, y \in \mathbb{Z}$.

<u>Proof</u>: ~~Sol~~ Proof by contradiction. Suppose $x, y \in \mathbb{Z}$ satisfy $x^3 + x = 4y^2 + 7$.

Then $x^3 + x + 1 = (4y^2 + 7) + 1 = 4y^2 + 8 = 4 \cdot (y^2 + 2)$
$\equiv 0 \mod 4$.

This is a contradiction because the congruence $x^3+x+1 \equiv 0 \bmod 4$ has no solutions (by part (a)). $\square$.

16. A positive integer n is <u>prime</u> if $n>1$ and the only positive integers which divide n are 1 and n itself.

a) <u>FTA</u>: For all positive integers n such that $n>1$, n can be written as a product of primes in a unique way (up to reordering the factors).

b) In general, if $n \in \mathbb{N}, n>1$, and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the prime factorizations of n, then the positive integers d such that $d \mid n$ are give by $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$ where $0 \leq \beta_i \leq \alpha_i$ for each $i = 1, \ldots, r$.

For $108 = 2 \cdot 54 = 2 \cdot 2 \cdot 27 = 2^2 \cdot 3^3$,

we have $d = 2^{\alpha_1} 3^{\alpha_2}$ where $0 \leq \alpha_1 \leq 2$ and $0 \leq \alpha_2 \leq 3$,

so $d = 1, 2, 4, \; 3, 6, 12, \; 9, 18, 36, \; 27, 54, 108$

c) By part b), $\#\{d \in \mathbb{N} \mid d \mid n\}$

$$= \#\{(\beta_1, \ldots, \beta_r) \in \mathbb{Z}^r \mid 0 \leq \beta_i \leq \alpha_i \text{ for each } i = 1, \ldots, r\}$$

$$= (\alpha_1+1) \cdot (\alpha_2+1) \cdots (\alpha_r+1).$$

17. <u>Claim</u>. For all $a, b \in \mathbb{N}$, if $a^2 \mid b^2$ then $a \mid b$.

<u>Proof</u>: Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$

be the prime factorizations of a & b.

(Note: here we allow α_i or $\beta_i = 0$ for some i so that we can use the same set of primes $p_1, \ldots, p_r$ for a & b.)

Then $a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$ & $b^2 = p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_r^{2\beta_r}$

So $a^2 \mid b^2 \iff 2\alpha_i \le 2\beta_i$ for each $i = 1, \ldots, r$

$\iff \alpha_i \le \beta_i$ for each $i = 1, \ldots, r$

$\iff a \mid b$. $\square$.

18. $f: A \to B$ is <u>injective</u> (or <u>one-to-one</u>) if

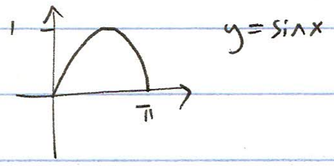
for all $a_1, a_2 \in A$, $(a_1 \ne a_2) \Rightarrow (f(a_1) \ne f(a_2))$

(Equivalently, $(f(a_1) = f(a_2)) \Rightarrow (a_1 = a_2)$).

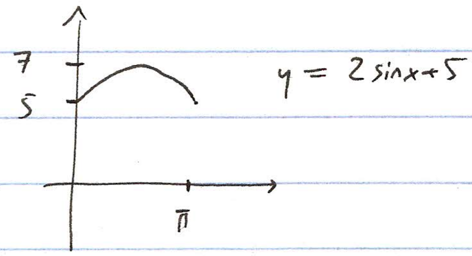
$f: A \to B$ is <u>surjective</u> (or <u>onto</u>) if for all $b \in B$,

there is an $a \in A$ such that $f(a) = b$.

a. $f: [0, \pi] \to \mathbb{R}$, $f(x) = 2\sin x + 5$.



$\leadsto$

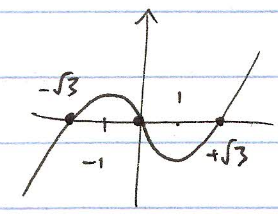


NOT injective : e.g. $f(0) = f(\pi) = 5$

NOT surjective : $|\sin x| \le 1 \Rightarrow$ ~~$|f(x)|$~~ $3 \le f(x) \le 7$

(More precisely, for $0 \le x \le \pi$, $0 \le \sin x \le 1 \Rightarrow 5 \le f(x) \le 7$, range$(f) = [5, 7]$)

b. $f: \mathbb{R} \to \mathbb{R}$ $f(x) = x^3 - 3x$



$f'(x) = 3x^2 - 3 = 3(x^2 - 1)$. $f'(x) = 0 \iff x = \pm 1$.

See f NOT injective. e.g. $f(x) = 0 \iff x \cdot (x^2 - 3) = 0$

$\iff x = 0, \pm\sqrt{3}$.

$\lim_{x\to\infty} f(x) = \infty$, $\lim_{x\to-\infty} f(x) = -\infty$, & f is continuous.

$\Rightarrow$ f is surjective (by intermediate value theorem)

c. $f: \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = x^2+y^2$

<u>NOT injective</u>: $f(x_1,y_1) = f(x_2,y_2) \iff x_1^2+y_1^2 = x_2^2+y_2^2$

$\iff (x_1,y_1)$ & (x_2,y_2) are same distance from $(0,0)$.

e.g. $f(1,0) = f(0,1)$.

<u>NOT surjective</u>: $f(x,y) = x^2+y^2 \geq 0$ for all x,y.

d. $f: \mathbb{N}^3 \to \mathbb{N}$ $f(x,y,z) = 2^x \cdot 3^y \cdot 5^z$.

<u>Injective</u>: by FTA : If $n = 2^{x_1}3^{y_1}5^{z_1} = 2^{x_2}3^{y_2}5^{z_2}$
then $(x_1,y_1,z_1) = (x_2,y_2,z_2)$
by uniqueness of prime factorizations.

<u>NOT surjective</u>: by FTA, only $n \in \mathbb{N}$ such that the prime factorization of n involves the prime factors $2,3,5$ and no other primes are in the range of f.

19. a. $f: \mathbb{Z}^2 \to \mathbb{Z}$ $f(x,y) = ax+by$.

The equation $ax+by=c$ has a solution $x,y\in\mathbb{Z}$ iff $\gcd(a,b) \mid c$.

So f is surjective $\iff \gcd(a,b) \mid c$ for all $c \in \mathbb{Z}$.

$\iff \gcd(a,b) = 1$.

b. f is NOT injective

because for all $x,y\in\mathbb{Z}$ and $t\in\mathbb{Z}$ ~~$f(x+tb, y-ta) = f(x,y)$~~

$f(x+tb, y-ta) = f(x,y)$

20 a. $f(x_1) = f(x_2) \iff ax_1 \equiv ax_2 \mod M$

$\iff M \mid ax_1 - ax_2 = a(x_1 - x_2)$

$\Rightarrow M \mid (x_1 - x_2)$ (using $\gcd(a, M) = 1$)

$\iff x_1 \equiv x_2 \mod M$

$\iff x_1 = x_2$ (using $x_1, x_2 \in \{0, 1, \ldots, M-1\}$)

So f is injective.

b. If A & B are finite sets such that $|A| = |B|$ and f is a function from A to B then f is injective iff f is surjective :-

f injective $\iff |\text{range}(f)| = |A|$

$\iff \text{range}(f) = B$ (because $\text{range}(f) \subset B$ & $|A| = |B|$)

$\iff f$ surjective.

(This is sometimes called the "pigeonhole principle").

In our case, $f : A \to A$, $|A| = |A| = M$, f injective $\Rightarrow f$ surjective.

So f is bijective (= injective AND surjective)

21. $f : A \to B$ has an inverse $\iff f$ is bijective

a. $f : \mathbb{R} \to [5, \infty)$, $f(x) = 4e^x + 5$.

$f(x) > 5$ for all $x \in \mathbb{R}$ (because $e^x > 0$), so f is NOT surjective, f does NOT have an inverse

b. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 3x + 8$, $f(x) \equiv 8 \equiv 2 \mod 3$ for all $x \in \mathbb{Z}$, so f is NOT surjective, f does NOT have an inverse.

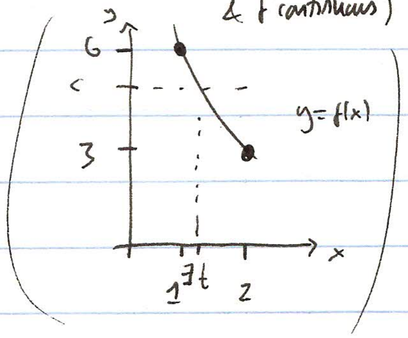
c. $f : [1, 2] \to [3, 6]$, $f(x) = x^2 - 6x + 11$.

$f'(x) = 2x - 6 < 0$ for $x \in [1, 2]$

So f is decreasing $\Rightarrow f$ is injective.
(using Mean Value Thm)

$f: [1,2] \longrightarrow [3,6]$

$f(1) = 6$, $f(2) = 3$ (& f continuous) $\Rightarrow$ f surjective by intermediate value theorem.



So f is bijective, f has an inverse.

To find explicit formula for inverse, write $f(x) = y$ & solve for x in terms of y (then $x = f^{-1}(y)$):-

$$x^2 - 6x + 11 = y$$

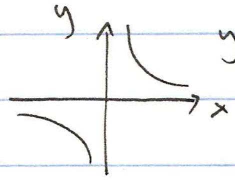
$$x^2 - 6x + (11-y) = 0$$

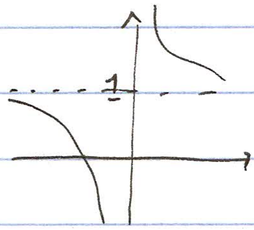
$$x \underset{QF}{=} \frac{-(-6) \pm \sqrt{36 - 4(11-y)}}{2} = \frac{6 \pm \sqrt{4y-8}}{2} = 3 \pm \sqrt{y-2}$$

$x \in [1,2] \Rightarrow$ sign is "$-$", $x = 3 - \sqrt{y-2}$.

$f^{-1}(y) = 3 - \sqrt{y-2}$, $\quad f^{-1}: [3,6] \longrightarrow [1,2]$.

d. $f: \mathbb{R}\setminus\{0\} \longrightarrow \mathbb{R}$, $\quad f(x) = 1 + \frac{1}{x}$





$1/x \neq 0$ for all $x \in \mathbb{R}\setminus\{0\}$ $\Rightarrow$ $f(x) \neq 1 \; \forall x \in \mathbb{R}\setminus\{0\}$

$\Rightarrow$ f NOT surjective,

f does NOT have an inverse.

e. $f: (0,\infty) \longrightarrow \mathbb{R}$

$f(x) = x - 1/x$

$f'(x) = 1 + 1/x^2 > 0$ for all $x \in (0,\infty)$ $\Rightarrow$ f increasing (by MVT)

$\Rightarrow$ f injective.

$\lim\limits_{x \to \infty} f(x) = \infty$, $\quad \lim\limits_{x \to 0^+} f(x) = -\infty$, f continuous

$\Rightarrow$ f surjective (by IVT)

So f is bijective, f has an inverse.

Explicit formula: $f(x) = y \iff x = f^{-1}(y)$.

$x - 1/x = y \iff x^2 - 1 = x \cdot y$ (note: $x \neq 0$)

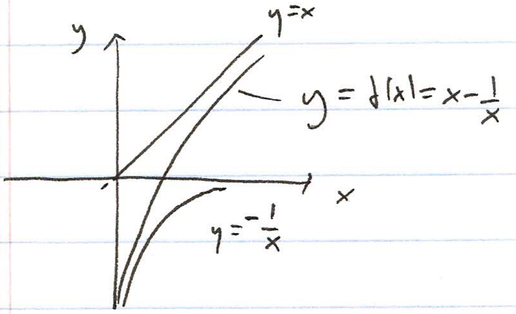
$\iff x^2 - y \cdot x - 1 = 0$

$\underset{QF}{\iff} x = \dfrac{y \pm \sqrt{y^2+4}}{2}$

$x \in (0,\infty) \Rightarrow$ sign is "+", (note $\sqrt{y^2+4} > \sqrt{y^2} = |y|$)

$$\boxed{f^{-1}(y) = \frac{y + \sqrt{y^2+4}}{2}}$$

$f^{-1} : \mathbb{R} \longrightarrow (0,\infty)$.



22. a. $f : A \to B$, $g : B \to A$ $\quad g(f(x)) = x$ for all $x \in A$ $(*)$

f surjective.

<u>Claim</u>: $f(g(y)) = y$ for all $y \in B$.

<u>Proof</u>: f surjective $\Rightarrow y = f(x)$ for some $x \in A$

$\Rightarrow f(g(y)) = f(\underbrace{g(f(x))}_{\overset{\shortparallel}{x} \text{ by } (*)}) = f(x) = y$. $\square$

b. $f : \underset{\overset{\shortparallel}{[0,\infty)}}{\mathbb{R}_{\geq 0}} \to \mathbb{R}$, $f(x) = \sqrt{x}$

$g : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$, $g(y) = y^2$

$g(f(x)) = (\sqrt{x})^2 = x \quad \forall x \in \mathbb{R}_{\geq 0}$

$f(g(y)) = \sqrt{y^2} = |y| \neq y$ if $y < 0$.

23. a. $|A| = m$, $|B| = n$

\# functions $f: A \to B$? $\quad A = \{a_1, a_2, \dots, a_m\}$

n choices for $f(a_1)$, n choices for $f(a_2)$, .., n choices for $f(a_m)$

$\Rightarrow$ n^m choices for f.

b. \# injective functions $f: A \to B$?

If $n < m$, no such functions. (because, for $f: A \to B$ a function, $\mathrm{range}(f) \subset B$
$\Rightarrow |\mathrm{range}(f)| \leq |B| < |A|$
$\Rightarrow f$ not injective)

If $n \geq m$:-

n choices for $f(a_1)$, $(n-1)$ choices for $f(a_2)$, .., $(n-m+1)$ choices for $f(a_m)$

$\Rightarrow$ $n \cdot (n-1) \cdot \dots (n-m+1) = n! / (n-m)!$ choices for f.

c). We use the hint.

$\#\{\text{surjective functions } f: A \to B\}$

$= |S \setminus S_1 \cup \dots \cup S_n|$

$= |S| - |S_1 \cup \dots \cup S_n|$

$= |S| - \sum_{1 \leq i \leq n} |S_i| + \sum_{1 \leq i < j \leq n} |S_i \cap S_j| - \sum_{1 \leq i < j < k \leq n} |S_i \cap S_j \cap S_k| + \dots + (-1)^n |S_1 \cap \dots \cap S_n|$

$= n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \dots + (-1)^n \binom{n}{n}(n-n)^m$

$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m \quad (*)$

Note that
$|S_{i_1} \cap S_{i_2} \cap \dots \cap S_{i_k}| = (n-k)^m$
for $1 \leq i_1 < i_2 < \dots < i_k \leq n$, because LHS
$= \#$ functions $f: A \to B \setminus \{b_{i_1}, b_{i_2}, \dots, b_{i_k}\}$
$=$ RHS by part a.

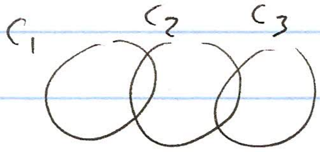
If $m < n$ then there are no surjective functions $f: A \to B$ (because $|\mathrm{range}(f)| \leq |A| < |B|$
$\Rightarrow \mathrm{range}(f) \neq B$), but this is not obvious from the formula $(*)$

24. a. R is <u>not</u> an equivalence relation because it is <u>not</u> transitive:-

$$C_1 R C_2 \ \& \ C_2 R C_3 \not\Rightarrow C_1 R C_3$$

$$C_1 \cap C_2 \neq \emptyset \ \& \ C_2 \cap C_3 \neq \emptyset \not\Rightarrow C_1 \cap C_3 \neq \emptyset$$

<u>Ex</u>:



$C_1 \cap C_2 \neq \emptyset$ & $C_2 \cap C_3 \neq \emptyset$, but $C_1 \cap C_3 = \emptyset$.

b. R is an equivalence relation:- Must check

1. Reflexive $\forall a \in S \quad aRa$
2. Symmetric: $\forall a, b \in S \quad aRb \Rightarrow bRa$
3. Transitive: $\forall a, b, c \in S \quad aRb$ AND $bRc \Rightarrow aRc$

1. It's possible to travel from a city a to itself by land (no travel required!)
2. If one can travel from a to b by land, then, reversing the route, one can travel from b to a by land.
3. If one can travel from a to b by land, and from b to c by land then one can travel from a to c by land by combining the two routes (travelling from a to b to c).

c. R is an equivalence relation:-

1. $\forall a \in S \quad aRa$: $\quad \frac{a}{a} = 1 = 1^2, \quad 1 \in \mathbb{Q}$.
2. $\forall a, b \in S \quad aRb \Rightarrow bRa$: If $a/b = t^2, \ t \in \mathbb{Q}$ then $b/a = (1/t)^2, \ 1/t \in \mathbb{Q}$ (note $t \neq 0$ because $a, b \in S = \mathbb{N}$)
3. $\forall a, b, c \in S \quad aRb$ AND $bRc \Rightarrow aRc$:

If $a/b = t^2$ and $b/c = u^2$, $t, u \in \mathbb{Q}$,
then $a/c = a/b \cdot b/c = t^2 u^2 = (tu)^2, \quad tu \in \mathbb{Q}$ $\square$.

25 No, R is not an equivalence relation.

If R is an equivalence relation on a set S, then the equivalence classes $[a] = \{x \in S \mid xRa\}$ for $a \in S$ form a partition of S.

In our example: $[1] = \{1,4,5\}$, $[2] = \{2,6\}$, $[3] = \{3,5\}$, $[4] = \{1,4,5\}$, $[5] = \{1,3,4,5\}$, & $[6] = \{2,6\}$.

These do not form a partition (because for example $[1] \cap [3] = \{5\} \neq \emptyset$ but $[1] \neq [3]$).

So R is not an equivalence relation.

Alternatively, R is not transitive, because for example $1R5$ and $5R3$ but $1 \not R 3$.

26 a) R is reflexive $\iff$ R contains the line $y=x$

R is symmetric $\iff$ $R = f(R)$, where $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x,y) = (y,x)$ is reflection in the line $y=x$.

b) Suppose $R \subset \mathbb{R}^2$, R contains the line $y = x+1$, and R is an equivalence relation on $\mathbb{R}$.

So $xR(x+1)$ $\forall x \in \mathbb{R}$.

$\therefore$ Using transitivity & induction, $xR(x+n)$ $\forall x \in \mathbb{R}$ and $n \in \mathbb{N}$

Also xRx $\forall x \in \mathbb{R}$ (reflexive) and, by symmetry

$(x+n)Rx$ $\forall x \in \mathbb{R}$ and $n \in \mathbb{N}$, equivalently, $xR(x-n)$ $\forall x \in \mathbb{R}$ and $n \in \mathbb{N}$.

Combining, $xR(x+n)$ $\forall x \in \mathbb{R}$ and $n \in \mathbb{Z}$.

i.e. $(xRy) \Leftarrow (y - x \in \mathbb{Z}.)$

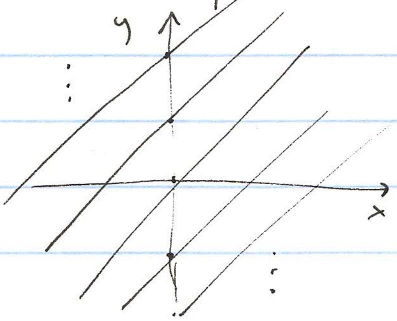
Conversely, if we define a relation R' on $S = \mathbb{R}$ by

$$xR'y \iff y - x \in \mathbb{Z}$$

then R' is an equivalence relation (checked in class / Exercise).

So R' is the smallest equivalence relation containing the line $y = x+1$.

Sketch of $R' \subset \mathbb{R}^2$:



R' = the union of the lines $y = x+n$, $n \in \mathbb{Z}$.

27 a. Yes:— Write $R = R_1 \cap R_2$. Note $aRb \iff aR_1b$ & aR_2b

1. (Reflexive) $\forall a \in S$. aR_1a & $aR_2a \implies aRa$
2. (Symmetric) $\forall a,b \in S$. $\left.\begin{array}{l} aR_1b \implies bR_1a \\ aR_2b \implies bR_2a \end{array}\right\} \implies (aRb \implies bRa)$
3. (Transitive) $\forall a,b,c \in S$. $\left.\begin{array}{l} aR_1b \;\&\; bR_1c \implies aR_1c \\ aR_2b \;\&\; bR_2c \implies aR_2c \end{array}\right\} \implies (aRb \;\&\; bRc \implies aRc)$

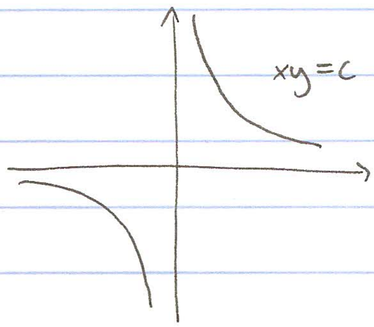
b. No. Write $R = R_1 \cup R_2$. Note $aRb \iff aR_1b$ OR aR_2b

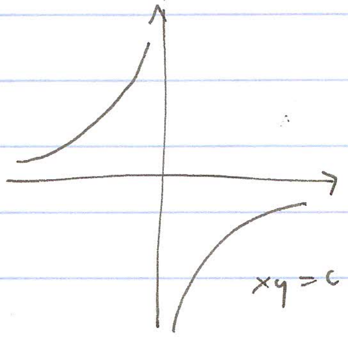
Transitivity will fail in general because we could have aR_1b and bR_2c but $a \not R_1 c$ and $a \not R_2 c$, so that aRb and bRc but $a \not R c$.

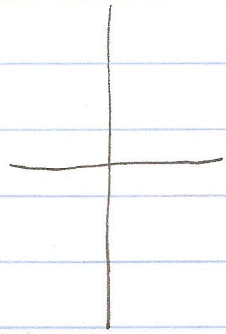
<u>Ex</u>: $\left.\begin{array}{l} R_1 = \text{congruence modulo } 2 \\ R_2 = \text{congruence modulo } 3 \end{array}\right\}$ on $S = \mathbb{Z}$.

$2R_10$ and $0R_23$ but $2\not R_1 3$ and $2 \not R_2 3$.

28.







(The equivalence classes of R on $\mathbb{R}^2$ are the curves $f(x,y) = c$, where $c \in \mathbb{R}$ is a constant.)

29. a) $A = \{n \in \mathbb{Z} \mid n \geq -4\}$ is countable:

$f : \mathbb{N} \longrightarrow A$ $\quad f(n) = n - 5$ is a bijection.

b). $A = \{n \in \mathbb{Z} \mid n \equiv 3 \bmod 5\} = \{n \in \mathbb{Z} \mid n = 5q + 3, \text{ some } q \in \mathbb{Z}\}$

So, we have a bijection $f: \mathbb{Z} \longrightarrow A$
$f(q) = 5q+3$

Also, we have a bijection $g: \mathbb{N} \longrightarrow \mathbb{Z}$
(HW8Q5)

Composing gives a bijection $f \circ g: \mathbb{N} \longrightarrow A$.
So A is countable.

c) $A = \{p \in \mathbb{N} \mid p \text{ is prime}\}$ is a subset of $\mathbb{N}$,
so it is countable.
(In general, a subset of a countable set is countable)

d) $A = \mathbb{Q} \times \mathbb{Q}$.
$\mathbb{Q}$ is countable : $\exists$ $f: \mathbb{N} \longrightarrow \mathbb{Q}$ bijection (proved in class).
So we have a bijection $g: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q} \times \mathbb{Q}$
$g(n,m) = (f(n), f(m))$
$\mathbb{N} \times \mathbb{N}$ is countable : $\exists$ $h: \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ bijection (proved in class)
So, composing, we have a bijection $g \circ h : \mathbb{N} \longrightarrow \mathbb{Q} \times \mathbb{Q}$.
So $\mathbb{Q} \times \mathbb{Q}$ is countable.

e) $A = (0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$
A is uncountable :-
<u>Either</u> use Cantor's diagonal argument (using decimal expansion)
as in class to give a proof by contradiction
<u>Or</u> describe a bijection $f: (0,1) \longrightarrow \mathbb{R}$
for example $f(x) = \tan\left(\frac{\pi}{2} \cdot (2x-1)\right)$
Then $\mathbb{R}$ uncountable (proved in class) $\Rightarrow$ $(0,1)$ uncountable.

f. $A = \mathbb{R} \setminus \mathbb{Q} = \{ x \in \mathbb{R} \mid x \text{ is irrational} \}$

Notice $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$.

$\mathbb{R}$ is uncountable & $\mathbb{Q}$ is countable

So $\mathbb{R} \setminus \mathbb{Q}$ is uncountable :-

we showed in class that if A and B are countable, then $A \cup B$ is countable. The contrapositive of this statement is: if $A \cup B$ is uncountable then A or B is uncountable. $\square$