P1

Math A : Assignment one

1. $A = \{1, 2, 3\}$, $B = \{1, 3\}$.

$P(A) = \{\phi, A, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\}$.

$P(B) = \{\phi, B, \{1\}, \{3\}\}$.

$m(A) = 3$, $m(B) = 2$.

$m(P(A)) = 2^3$. $m(P(B)) = 2^2$.

$\Rightarrow$ if $m(X) = n$, then $m(P(X)) = 2^n$.

$A - B = \{2\}$,

$P(A-B) = \{\phi, A-B\}$.

p2

$P(A) - P(B) = \{ \{2\}, \{1,2\}, \{1,3\}, \{2,3\}, A \}$

$P(\{\phi\}) = \{ \{\phi\}, \{\phi\} \} = \{ \{\phi\} \}$.

error: $\{\phi\}$ is changed by $\phi$. then $P(\{\phi\}) = \{\phi, \{\phi\}\}$.

2. $X = \{ x^2 \mid x \in \mathbb{Z} \}$

$\hat{X} = \{ x \in \mathbb{R} \mid x < 1 \} = \{ x < 1 \mid x \in \mathbb{R} \}$ ← forget about this notation.

3. $A = \{1,2,3,4\}$, $B = \{1,2\}$.

$A \times B = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,2), (4,1), (4,2)\}$.

$B \times A = \{(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4)\}$.

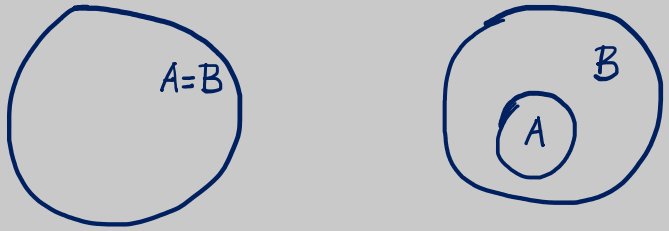
$A \times B - B \times A = \{(3,1), (3,2), (4,1), (4,2)\}$.

P3.

4. Let $A, B$ and $C$ be subsets of universe $U$.

(a) $(A \cup B) \subseteq B$.

From $B \subseteq A \cup B$., it follows that $A \cup B = B$, then $A \subseteq B$.




(b) $A \subseteq B$, $A \subseteq C$, $(B \cap C) \subseteq A$.

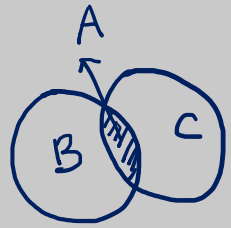
From $A \subseteq B$ and $A \subseteq C$, we know that

$\forall a \in A$, $a \in B \cap C$,

this gives $A \subseteq B \cap C$.

Together with $(B \cap C) \subseteq A$,

we find $A = B \cap C$.

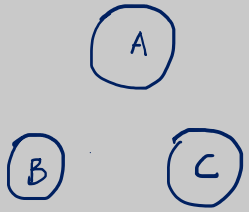



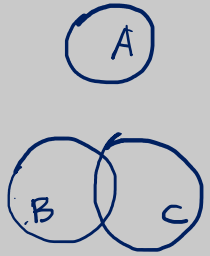
P4.

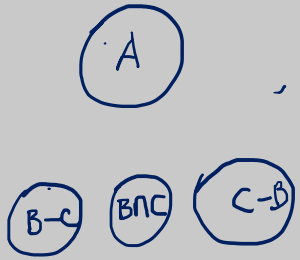
5. (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

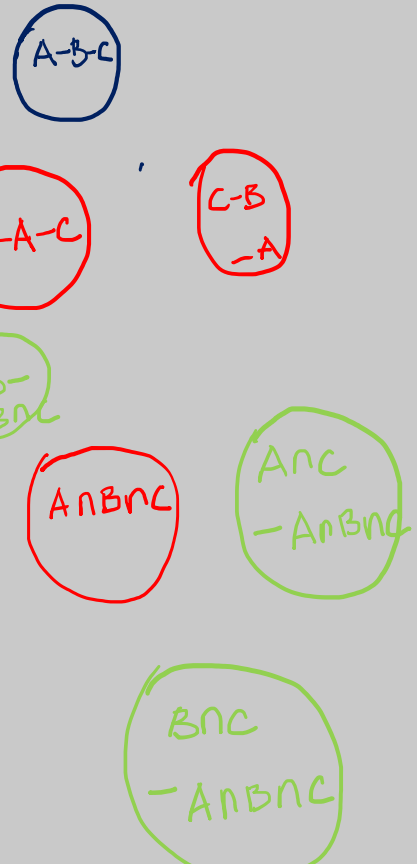
④ 

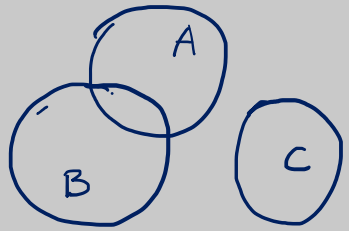
⇔

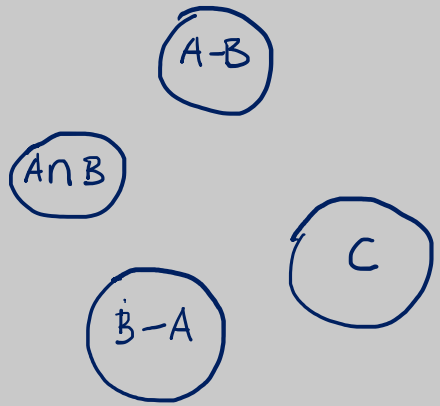
① 


② 

⇔



③ 

⇔


5. (a) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

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

proof $\Rightarrow$ If $\forall$ $a \in A \cap (B \cup C)$, then $a \in A$ and $[a \in B$ or $a \in C]$,

which is to say $[a \in A$ and $a \in B]$ or $[a \in A$ and $a \in C]$.

Then we rewrite the relation by

$a \in (A \cap B \quad \cup \quad a \in A \cap C$

$\Leftarrow$ If $\forall$ $a \in (A \cap B) \cup (A \cap C)$, then $a \in (A \cap B)$ or $a \in A \cap C$. This implies that $[a \in A$ and $a \in B]$ or $[a \in A$ and $a \in C]$, which is

$a \in A$ and $[a \in B$ or $a \in C]$.

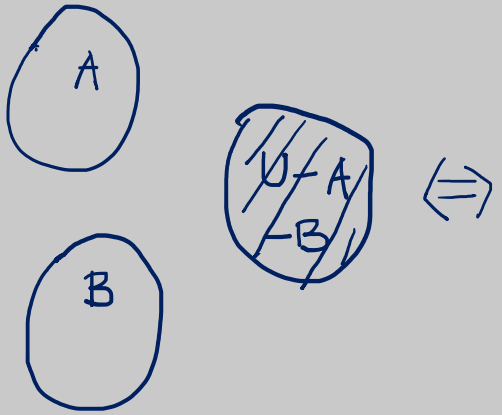
P6.

6. (a) $A, B$ are two generic sets, Prove

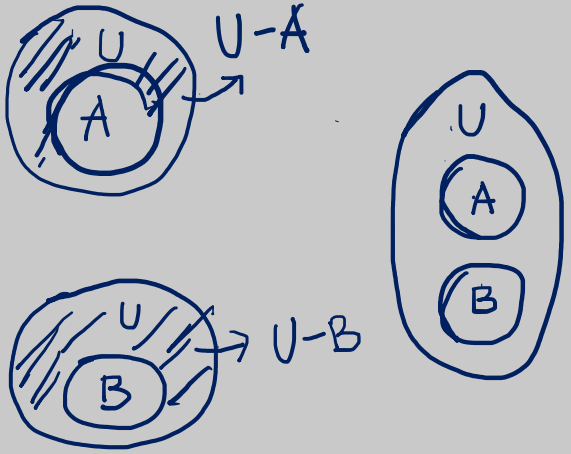
$$(A \cap B)^c = A^c \cap B^c$$

proof: $(A \cap B)^c \subseteq A^c \cap B^c$

$(A \cap B)^c \supseteq A^c \cap B^c$




$\Leftrightarrow$




$U - A - B$

$= (U - A) \cup (U - B)$

$= (U - A - B) \cup (A \cap B)$

$\Rightarrow$: $\forall\ a \in (A \cap B)^c$, $a \notin A \cap B$, which is $a \notin A$ or $a \notin B$

$a \in A^c$ or $a \in B^c$. This is to say $a \in A^c \cup B^c$.

$\Leftarrow$: If $\forall\ a \in A^c \cup B^c$, then $a \in A^c$ or $a \in B^c$.

$a \notin A$ or $a \notin B$. This means $a \notin A \cap B$ or

$a \notin A \cap B$. Then $a \in (A \cap B)^c$.

**Mathematics A**
Assignment two / Solutions

---

**1.** Let $U$ be a set and let $\mathcal{F}_1$ and $\mathcal{F}_2$ be nonempty families of subsets of $U$ such that $\mathcal{F}_1 \subseteq \mathcal{F}_2$. Show (=prove) that the following inclusions hold:

(a) $\bigcup \mathcal{F}_1 \subseteq \bigcup \mathcal{F}_2$
(b) $\bigcap \mathcal{F}_2 \subseteq \bigcap \mathcal{F}_1$

*Solution.* (a) Let $x \in \bigcup \mathcal{F}_1$. This means that there is $A \in \mathcal{F}_1$ such that $x \in A$. Because $\mathcal{F}_1 \subseteq \mathcal{F}_2$, there exists $A \in \mathcal{F}_2$ such that $x \in A$. Therefore, $x \in \bigcup \mathcal{F}_2$ and the claim is proved.
(b) We prove $\left(\bigcap \mathcal{F}_1\right)^c \subseteq \left(\bigcap \mathcal{F}_2\right)^c$. This is equivalent to the original claim, but is easier to prove. As it is written is the lecture notes: "$A \subseteq B$ can be sometimes shown easier by showing that $B^c \subseteq A^c$". Assume that $x \in \left(\bigcap \mathcal{F}_1\right)^c$. This means that $x \notin \bigcap \mathcal{F}_1$. So, there is $A \in \mathcal{F}_1$ such that $x \notin A$. Since $\mathcal{F}_1 \subseteq \mathcal{F}_2$, there is $A \in \mathcal{F}_2$ such that $x \notin A$. Therefore, $x \notin \bigcap \mathcal{F}_1$ and $x \in \left(\bigcap \mathcal{F}_2\right)^c$. The claim is proved.

**2.** Let $U$ be a set and let $\emptyset \neq \mathcal{F} \subseteq \wp(U)$ be a nonempty family of subsets of $U$. Prove the following equalities:

(a) $\left(\bigcap \mathcal{F}\right)^c = \bigcup \{A^c \mid A \in \mathcal{F}\}$
(b) $\left(\bigcup \mathcal{F}\right)^c = \bigcap \{A^c \mid A \in \mathcal{F}\}$

Recall that the complement of any $X \subseteq U$ is defined by $X^c = U \setminus X$.

*Solution.* Let $x \in U$.

$$x \in \left(\bigcap \mathcal{F}\right)^c \iff x \notin \bigcap \mathcal{F} \iff (\exists A \in \mathcal{F})\, x \notin A \iff (\exists A \in \mathcal{F}) x \in A^c \iff x \in \bigcup \{A^c \mid A \in \mathcal{F}\}.$$

This proves (a). Case (b) is rather similar:

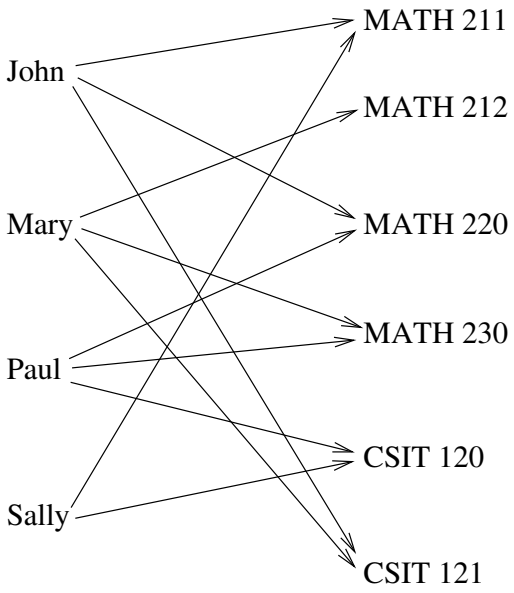
$$x \in \left(\bigcup \mathcal{F}\right)^c \iff x \notin \bigcup \mathcal{F} \iff (\forall A \in \mathcal{F})\, x \notin A \iff (\forall A \in \mathcal{F}) x \in A^c \iff x \in \bigcap \{A^c \mid A \in \mathcal{F}\}.$$

**3.** The courses taken by John, Mary, Paul, and Sally are listed below:

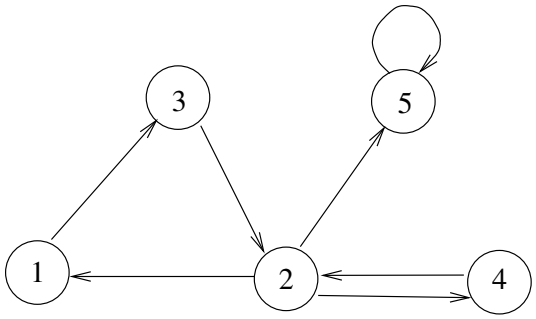
John: MATH 211, CSIT 121, MATH 220
Mary: MATH 230, CSIT 121, MATH 212
Paul: CSIT 120, MATH 230, MATH 220
Sally: MATH 211, CSIT 120

Give a graphical representation of the relation $R$ defined as $a\,R\,b$ if student $a$ is taking course $b$.

*Solution.*



**4.** Write the set of ordered pairs for the relation represented by the following directed graph:




*Solution.*

$$\{(1,3),(2,1),(2,4),(2,5),(3,2),(4,2),(5,5)\}$$

**5.** Let $R$ be a binary relation on the set $\wp(\{a,b\})$ defined so that $(A,B) \in R$ holds if $A \cap B = \emptyset$. Write out the relation $R$.

*Solution.*

$$R = \{(\emptyset,\emptyset),(\emptyset,\{a\}),(\emptyset,\{b\}),(\emptyset,\{a,b\}),(\{a\},\emptyset),(\{b\},\emptyset),(\{a,b\},\emptyset),(\{a\},\{b\}),(\{b\},\{a\})\}$$

**6.** Let $A$, $B$, $C$ be sets. Prove the following equalities:

(a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
(b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

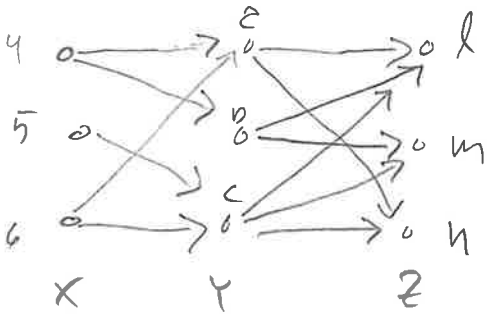
*Solution.* We show that the elements in left-hand side are the same as the elements in the right-hand side.

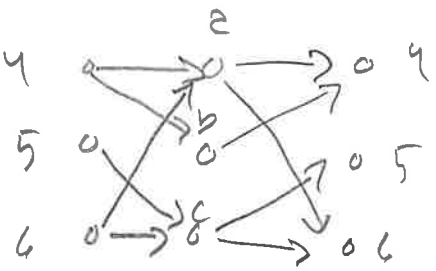
$$(a,b) \in A \times (B \cap C) \iff a \in A \text{ and } b \in (B \cap C) \iff a \in A \text{ and } (b \in B \text{ and } b \in C)$$
$$\iff (a \in A \text{ and } b \in B) \text{ and } (a \in A \text{ and } b \in C) \iff (a,b) \in A \times B \text{ and } (a,b) \in A \times C$$
$$\iff (a,b) \in (A \times B) \cap (A \times C).$$

This proves (a). The proof for (b) is similar:

$$(a,b) \in A \times (B \cup C) \iff a \in A \text{ and } b \in (B \cup C) \iff a \in A \text{ and } (b \in B \text{ or } b \in C)$$
$$\iff (a \in A \text{ and } b \in B) \text{ or } (a \in A \text{ and } b \in C) \iff (a,b) \in A \times B \text{ or } (a,b) \in A \times C$$
$$\iff (a,b) \in (A \times B) \cup (A \times C).$$

(1)




$R \circ S = \{(4,l), (4,m), (4,n), (5,l), (5,m), (5,n), (6,l), (6,m), (6,n)\} = \underline{X \times Z}$

$R^{-1} = \{(a,4), (b,4), (c,5), (a,6), (c,6)\}$

$R \circ R^{-1} = \{(4,4), (4,6), (5,5), (5,6), (6,4), (6,5), (6,6)\}$

---

(2) a) $T = \{(x, x^2) \mid x \in \mathbb{R}^+\}$

$T^{-1} = \{(x, \sqrt{x}) \mid x \in \mathbb{R}^+\}$

b) $S = \{(x, 3x-1) \mid x \in \mathbb{R}\}$

$S^{-1} = \{(x, \frac{(x+1)}{3} \mid x \in \mathbb{R}\}$

---

(3) a) $G = P \circ P$

b) $S = P^{-1} \circ P$

c) $C = P^{-1} \circ P^{-1} \circ P \circ P$

④ Let $a \in A$ and $b \in B$. Then,

$(a,b) \in (R \cup S)^{-1} \Leftrightarrow (b,a) \in (R \cup S) \Leftrightarrow (b,a) \in R$ or $(b,a) \in S$

$\Leftrightarrow (a,b) \in R^{-1}$ or $(a,b) \in S^{-1} \Leftrightarrow (a,b) \in R^{-1} \cup S^{-1}$.

---

⑤ a)

| P | Q | P ∨ Q | P ⇒ Q | ¬P ⇒ Q |
|---|---|---|---|---|
| F | F | F | T | F |
| T | F | T | F | T |
| F | T | T | T | T |
| T | T | T | T | T |

b

| P | Q | P ∨ Q | P ∧ Q | ¬(P ∨ Q) | ¬(¬P ∨ ¬Q) |
|---|---|---|---|---|---|
| F | F | F | F | T | F |
| F | T | T | F | F | F |
| T | F | T | F | F | F |
| T | T | T | T | F | T |

---

⑥

| P | Q | (P ⇒ Q) | P ∨ Q | (P ⇒ Q) ⇒ Q |
|---|---|---|---|---|
| F | F | T | F | F |
| T | F | F | T | T |
| F | T | T | T | T |
| T | T | T | T | T |

**Mathematics A** Assignment four (week 40)

Group 1 (Wed 6/10, 10–12), Group 2 (Fri 8/10, 8–10), Group 3 (Fri 8/10, 12–14)

**1.**

(a) Suppose $P$ is FALSE, $Q$ is FALSE, $S$ is TRUE.

$$(S \vee P) \wedge (Q \wedge \neg S) = (\mathbf{T} \vee \mathbf{F}) \wedge (\mathbf{F} \wedge \neg \mathbf{T}) = \mathbf{T} \wedge \mathbf{F} = \mathbf{F}$$

(b) Suppose $P$ is TRUE, $Q$ is TRUE, $R$ is FALSE, $S$ is FALSE.

$$(Q \vee P) \wedge (\neg R \vee \neg S) = (\mathbf{T} \vee \mathbf{T}) \wedge (\neg \mathbf{F} \vee \neg \mathbf{F}) = \mathbf{T} \wedge \mathbf{T} = \mathbf{T}$$

**2.** Let $P$, $Q$, $R$ and $S$ be logical propositions.

(a) Suppose $P$ is FALSE, $S$ is FALSE, $R$ is TRUE.

$$\neg\big((S \wedge P) \vee \neg R\big) = \neg\big((\mathbf{F} \wedge \mathbf{F}) \vee \neg \mathbf{T}\big) = \neg(\mathbf{F} \vee \mathbf{F}) = \neg \mathbf{F} = \mathbf{T}.$$

(b) Suppose $P$ is TRUE, $Q$ is FALSE, $R$ is TRUE.

$$P \Rightarrow (Q \Leftrightarrow R) \;=\; \mathbf{T} \Rightarrow (\mathbf{F} \Leftrightarrow \mathbf{T}) \;=\; \mathbf{T} \Rightarrow \mathbf{F} = \mathbf{F}.$$

**3.**

(a)

| Div. by 2 | Quotient | Remainder |
|---|---|---|
| 79/2 | 39 | 1 |
| 39/2 | 19 | 1 |
| 19/2 | 9 | 1 |
| 9/2 | 4 | 1 |
| 4/2 | 2 | 0 |
| 2/2 | 1 | 0 |
| 1/2 | 0 | 1 |

$B = 100\,1111$

(b)

| Binary | 1 | 1 | 1 | | 1 | 1 | 1 | 0 | | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Position | 10 | 9 | 8 | | 7 | 6 | 5 | 4 | | 3 | 2 | 1 | 0 |

$$\begin{aligned} D &= 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 2^0 \\ &= 1024 + 512 + 256 + 64 + 32 + 4 + 1 = 2021 \end{aligned}$$

**4.** Let $U = \{a, b, c, d, e, f\}$.

(a) $\emptyset = (0, 0, 0, 0, 0, 0)$ and $U = (1, 1, 1, 1, 1, 1)$

(b) $A = (1, 0, 1, 1, 0, 1)$ and $B = (1, 1, 0, 0, 1, 1)$

(c) $A \cup B = (1 \vee 1, 0 \vee 1, 1 \vee 0, 1 \vee 0, 0 \vee 1, 1 \vee 1) = (1, 1, 1, 1, 1, 1)$ and
$A \cap B = (1 \wedge 1, 0 \wedge 1, 1 \wedge 0, 1 \wedge 0, 0 \wedge 1, 1 \wedge 1) = (1, 0, 0, 0, 0, 1)$.

(d) $A^c = (\neg 1, \neg 0, \neg 1, \neg 1, \neg 0, \neg 1) = (0, 1, 0, 0, 1, 0)$ and
$B \setminus A = (1 \wedge \neg 1, 1 \wedge \neg 0, 0 \wedge \neg 1, 0 \wedge \neg 1, 1 \wedge \neg 0, 1 \wedge \neg 1) = (0, 1, 0, 0, 1, 0)$

**5.** Now $x|y$ means that there is an integer $k$ such that $y = kx$. If $a|b$ and $b|c$, then there are integers $k_1$ and $k_2$ such that $b = k_1 a$ and $c = k_2 b$. This means that

$$c = k_2 b = k_2 k_1 a.$$

Because $k_1 k_2$ is an integer, $a|c$.

**6.** Let $P =$ "$ab$ is even". Then $\neg P =$ "$ab$ is **not** even", that is, $\neg P =$ "$ab$ is odd". Let $Q =$ "$a$ **or** $b$ is even". In fact, $Q$ consists of **two** propositions $Q_1 =$ "$a$ is even" and $Q_2 =$ "$b$ is even". Then, $Q = Q_1 \vee Q_2$ and

$$\begin{aligned}\neg Q = \neg(Q_1 \vee Q_2) = \neg Q_1 \wedge \neg Q_2 &= \text{"}a \text{ is } \textbf{not} \text{ even"} \wedge \text{"}b \text{ is } \textbf{not} \text{ even"} \\ &= \text{"}a \text{ is odd"} \wedge \text{"}b \text{ is odd"} = \text{"}a \text{ and } b \text{ are odd"}\end{aligned}$$

Then, the claim

If $ab$ is an even number, then $a$ or $b$ is even

equals the proposition $P \Rightarrow Q$.

(a) This proves $\neg Q \Rightarrow \neg P$. This is logically equivalent to $P \Rightarrow Q$. Therefore, the proof is valid.
(b) This proves $Q \Rightarrow P$. The proof is not valid.
(c) This supposes that $P$ is true. Then it shows that from $\neg Q$ follows the contradiction **F**. Therefore, $Q$ is true. We have that $P \Rightarrow Q$ is true and the proof is valid.
(d) This also supposes that $P$ is true. Then it shows that $\neg Q_1$ implies $Q_2$, that is, $\neg Q_1 \Rightarrow Q_2$. Now $\neg Q_1 \Rightarrow Q_2$ is equivalent to $Q_1 \vee Q_2$. Thus, $Q = Q_1 \vee Q_2$ is true and we have shown that $P \Rightarrow Q$ is true. The proof is valid.

**1.** ($\Rightarrow$) Let $A \subseteq B$. Assume for contradiciton that

$$A \setminus B = \{a \in U \mid a \in A \text{ and } a \notin B\} \neq \emptyset.$$

This means that there is $x \in A$ such that $x \notin B$. This is not possible, because $A \subseteq B$, a contradiction. Therefore, $A \setminus B = \emptyset$.

($\Leftarrow$) Assume $A \setminus B = \emptyset$. By the definition of the set difference, this means that there is no element $x \in U$ such that $x \in A$ and $x \notin B$. Hence, if $a \in A$, then $a \in B$ and $A \subseteq B$.

**2.** Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$. Which of the following relations are (i) functions, (ii) injections, (iii) surjections, (iv) bijections?

(a) $R_1 = \{(1, a), (2, c), (3, b), (4, d)\}$ is a bijection (all properties i-iv)
(b) $R_2 = \{(1, a), (2, b), (3, c), (4, c)\}$ is a function. Not injection, because 3 and 4 have the same image. Not surjection, because $d \in B$ is not an image of any element of $A$.
(c) $R_3 = \{(1, a), (2, b), (3, c), (3, d)\}$ is not a function, because $3 \in A$ is related to two elements in $B$.

**3.**

(a) $$2^{5x-2} = 16 \Leftrightarrow \log_2(2^{5x-2}) = \log_2 16 \Leftrightarrow 5x - 2 = 4 \Leftrightarrow 5x = 6 \Leftrightarrow x = \frac{6}{5}.$$

(b) $$5 \log_7 x = 10 \Leftrightarrow \log_7 x = 2 \Leftrightarrow 7^{\log_7 x} = 7^2 \Leftrightarrow x = 49.$$

(c) $$\log_2(3x - 7) = 5 \Leftrightarrow 2^{\log_2(3x-7)} = 2^5 \Leftrightarrow 3x - 7 = 32 \Leftrightarrow 3x = 39 \Leftrightarrow x = 13.$$

(b) $$\log_4 x + \log_4(x - 6) = 2 \Leftrightarrow \log_4(x(x - 6)) = 2 \Leftrightarrow \log_4(x^2 - 6x) = 2$$
$$\Leftrightarrow 4^{\log_4(x^2-6x)} = 4^2 \Leftrightarrow x^2 - 6x = 16 \Leftrightarrow x^2 - 6x - 16 = 0.$$

The last second degree polynomial has solutions $x = 8$ and $x = -2$, but $x = -2$ is not possible, because the "input" for logarithm-function needs to be positive. The only solution is therefore $x = 8$.

**4.** Suppose for the contradiction that there are integers $x$ and $y$ such that $x^2 = 4y+2$. Now $4y+2 = 2(2y+1)$ is an even number. This gives that $x^2$ is an even number and therefore (lectures!) $x$ is an even number. There is an integer $k$ such that $x = 2k$ and we have $x^2 = (2k)^2 = 4k^2 = 2(2y + 1)$. After division by 2, the last equality gives

$$2k^2 = 2y + 1.$$

This is impossible, because $2k^2$ is even and $2y + 1$ is odd, a contradiction! So, there are **no** integers $x$ and $y$ such that $x^2 = 4y + 2$.

**5.** We prove the contrapositive:

$$\neg(n \text{ is odd}) \implies \neg(5n \text{ is odd}),$$

that is,

$$n \text{ is even} \implies 5n \text{ is even}.$$

Assume $n$ is even. This means that there is an integer $k$ such that $n = 2k$. Now

$$5n = 5 \cdot 2k = 2 \cdot 5k$$

is also even.

**6.** Suppose for contradiction that $\log_{10}(7)$ is rational. This means that there are integers $a$ and $b \neq 0$ such that

$$\log_{10}(7) = \frac{a}{b}.$$

Because $\log_{10}(7) > 0$, we may assume that $a$ and $b$ are both positive integers. We have that $b \log_{10}(7) = a$ and $a = \log_{10}(7^b)$. This also gives

$$10^a = 10^{\log_{10}(7^b)} = 7^b.$$

Now

$$10^a = 2 \cdot 5 \cdot 10^{a-1},$$

which means that $10^a$ is even. Becuase 7 is odd, $7^b$ is odd. This is a contradiction (a number cannot be odd and even). Thus, $\log_{10}(7)$ is irrational.

**1.** One way to start is to see that $8 = 2^3$. Then we may observe that $343^{\frac{1}{3}} = 7$, that is, $7^3 = 343$. We can write:

$$\left(\frac{8}{343}\right)^{-\frac{2}{3}} = \left(\frac{2^3}{7^3}\right)^{-\frac{2}{3}} = \left(\frac{2}{7}\right)^{-3\cdot\frac{2}{3}} = \left(\frac{2}{7}\right)^{-2}.$$

We know that for all $x \in \mathbb{R}$,

$$x^{-2} = \left(\frac{1}{x}\right)^2.$$

Therefore,

$$\left(\frac{2}{7}\right)^{-2} = \left(\frac{7}{2}\right)^2 = \frac{49}{4}.$$

**2.** (a) (Case i) If $x \geq 1/4$, then $|4x - 1| = 4x - 1$. We have the solution.

$$4x - 1 = 3 \iff 4x = 4 \iff x = 1.$$

Now the solution $x = 1$ is in the right area $x \geq 1/4$
(Case ii) If $x < 1/4$, then $|4x - 1| = 1 - 4x$. We have the solution

$$1 - 4x = 3 \iff 4x = -2 \iff x = -\frac{1}{2}.$$

Also now the solution $x = -\frac{1}{2}$ is in the right area $x < 1/4$

(b) (Case i) If $x \geq -2$, then $|x + 2| = x + 2$. We get

$$x + 2 = \frac{1}{3}x + 5 \iff x - \frac{1}{3}x = 5 - 2 \iff \frac{2}{3}x = 3 \iff x = \frac{9}{2} = 4\frac{1}{2}.$$

The solution belongs to the area.
(Case ii) If $x < -2$, then $|x + 2| = -x - 2$. The solution is

$$-x - 2 = \frac{1}{3}x + 5 \iff x + \frac{1}{3}x = -7 \iff \frac{4}{3}x = -7 = x = -\frac{7 \cdot 3}{4} = -\frac{21}{4}.$$

The solution belongs to the area.

**3.** (Case i) If $x \geq 5/6$, then $|6x - 5| = 6x - 5$ and $|3x + 4| = 3x + 4$. The solution is

$$6x - 5 = 3x + 4 \iff x = 3$$

The solution belongs to the area.
(Case ii) If $-3/4 \leq x < 5/6$, then $|6x - 5| = 5 - 6x$ and $|3x + 4| = 3x + 4$. We can solve:

$$5 - 6x = 3x + 4 \iff x = \frac{1}{9}.$$

The solution belongs to the area.

(Case iii) if $x < -3/4$, then $|6x-5| = 5-6x$ and $|3x+4| = -3x-4$. The solution is

$$5-6x = -3x-4 \iff x = 3.$$

The solution does no belong to the area. But no worries, because we already have found this solution.

**4.** Let $A$, $B$, and $C$ be sets and suppose that there are bijections $f\colon A \to B$ and $g\colon B \to C$.
(i) We prove that $g \circ f\colon A \to C$ is a surjection. Let $c \in C$. Because $g$ is a bijection, it is a surjection. Therefore, there is $b \in B$ such that $g(b) = c$. Moreover, because $f$ is surjective, there is $a \in A$ such that $f(a) = b$. We have that

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

This means that $g \circ f$ is a surjection.

(ii) We prove that $g \circ f\colon A \to C$ is an injection. Suppose that $(g \circ f)(a) = (g \circ f)(b)$ for some $a, b \in A$, that is, $g(f(a)) = g(f(b))$. Because $g$ is a injection, we have $f(a) = f(b)$. Because $f$ is an injection, we get $a = b$.

Since $g \circ f$ is both surjective and injective, it is a bijection.

**5.** The solution is that each guest moves to the next room: guest in room 1 moves to room 2, guest in room 2 moves to room 3, guest in room 3 moves to room 4, and so on. Because the hotel is enumerable infinite, this can be done. The new guest can enter to room 1.

**6.** The solution is that the guest in room $k$ moves to the room $2k$. This means that all rooms with odd number get free: 1, 3, 5, 7, ... There are countable infinite number of new passengers:

$$x_0, x_1, x_2, x_3, \ldots$$

We can accommodate them in rooms having odds numbers by the rule (function) that the guest $x_k$ goes to the room $2k+1$.

**1.**

$$\binom{70}{5} = \frac{70!}{5!\,65!} = \frac{66 \cdot 67 \cdot 68 \cdot 69 \cdot 70}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 11 \cdot 67 \cdot 17 \cdot 69 \cdot 14 = 12103014$$

$$\binom{121}{115} = \frac{121!}{115!\,6!} = \frac{116 \cdot 117 \cdot 118 \cdot 119 \cdot 120 \cdot 121}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 116 \cdot 39 \cdot 59 \cdot 119 \cdot 121 = 3843323484.$$

**2.**

$$\begin{aligned}(1+x)^7 &= \binom{7}{0}x^7 + \binom{7}{1}x^6 + \binom{7}{2}x^5 + \binom{7}{3}x^4 + \binom{7}{4}x^3 + \binom{7}{5}x^2 + \binom{7}{6}x^1 + \binom{7}{7}x^0 \\ &= x^7 + 7x^6 + 21x^5 + 35x^4 + 35x^2 + 21x^2 + 7x + 1\end{aligned}$$

**3.** There are several ways to enumerate

$$F(\mathbb{N}) = \{X \subseteq \mathbb{N} \mid X \text{ is finite}\}.$$

(a) If $X = \{x_1, x_2, \ldots, x_n\}$ is a finite subset of $\mathbb{N}$, then the sum $x_1 + \cdots + x_n$ of its elements is a natural number. It is also clear that for each integer $n \in \mathbb{N}$, the number of sets $X$ such that sum of the elements of $X$ equals $n$ is finite: each such set belongs to $\wp(\{0, 1, 2, \ldots, n\})$, whose size is finite. Therefore, we start with $\emptyset$, then enumerate all sets whose sum of elements is 0: $\{0\}$; then we enumerate all sets whose sum of elements is 1: $\{0, 1\}$, $\{1\}$, then all sets whose sum is 2: $\{0, 2\}$, $\{2\}$, sets whose sum is 3: $\{0, 1, 2\}$, $\{0, 3\}, \{3\}$, and so.
Because each finite set is such that the sum of its elements is a natural number, each set is enumerated a some point. Also because the number of sets $X$ such that sum of the elements of $X$ equals $n$ is finite, we never get stuck.

(b) Both *finite subsets of* $\mathbb{N}$ and *natural numbers* can be encoded as finite-length binary vectors. For instance, the binary representation of 6 is 110. This corresponds the set $\{1, 2\}$ – the idea is that the rightmost bit corresponds to 0, second bit from right corresponds to 1, 3rd bit corresponds to 2, etc. The following is a bijection between finite sets and numbers:

| | | |
|---|---|---|
| $0 \leftrightarrow \emptyset$ | $6 \leftrightarrow 110 \leftrightarrow \{1, 2\}$ | $12 \leftrightarrow 1100 \leftrightarrow \{2, 3\}$ |
| $1 \leftrightarrow \{0\}$ | $7 \leftrightarrow 111 \leftrightarrow \{0, 1, 2\}$ | $13 \leftrightarrow 1101 \leftrightarrow \{0, 2, 3\}$ |
| $2 \leftrightarrow 10 \leftrightarrow \{1\}$ | $8 \leftrightarrow 1000 \leftrightarrow \{3\}$ | $14 \leftrightarrow 1110 \leftrightarrow \{1, 2, 3\}$ |
| $3 \leftrightarrow 11 \leftrightarrow \{0, 1\}$ | $9 \leftrightarrow 1001 \leftrightarrow \{0, 3\}$ | $15 \leftrightarrow 1111 \leftrightarrow \{0, 1, 2, 3\}$ |
| $4 \leftrightarrow 100 \leftrightarrow \{2\}$ | $10 \leftrightarrow 1010 \leftrightarrow \{1, 3\}$ | $16 \leftrightarrow 10000 \leftrightarrow \{4\}$ |
| $5 \leftrightarrow 101 \leftrightarrow \{0, 2\}$ | $11 \leftrightarrow 1011 \leftrightarrow \{0, 1, 3\}$ | $17 \leftrightarrow 10001 \leftrightarrow \{0, 4\}$ |

**4.** The map $f\colon \mathbb{Z} \to \mathbb{N}$ is defined by

$$f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -2n - 1 & \text{if } n < 0 \end{cases}$$

**Surjection:** Let $n \in \mathbb{N}$. If $n$ is *even*, then $n = 2k$ for some integer $k \geq 0$. We have $k = \frac{n}{2}$. Now $f(k) = 2 \cdot \frac{n}{2} = n$. If $n$ is *odd*, then $n = 2k - 1$ for some integer $k \geq 1$. Now $k = \frac{n+1}{2}$ and $-k = \frac{-n-1}{2}$. Because $k \geq 1$, $-k < 0$. We have that $f(-k) = -2 \cdot \frac{-n-1}{2} - 1 = n$.

**Injection:** If $n \geq 0$, then $f(n)$ is even and if $n < 0$, then $f(n)$ is odd. The means that if $f(n_1) = f(n_2)$, we have only two cases:

(i) $n_1 \geq 0$ and $n_2 \geq 0$: $f(n_1) = f(n_2)$ implies $2n_1 = 2n_2$ and $n_1 = n_2$.
(ii) $n_1 < 0$ and $n_2 < 0$: $f(n_1) = f(n_2)$ implies $-2n_1 - 1 = -2n_2 - 1$ and $n_1 = n_2$.

Because $f$ is injective and surjective, it is a bijection.

**5.** The map $f\colon (0,1) \to \mathbb{R}$ is defined by

$$f(x) = \begin{cases} \dfrac{1}{x} - 2 & \text{if } 0 < x \leq \dfrac{1}{2} \\ \dfrac{1}{x-1} + 2 & \text{if } \dfrac{1}{2} < x < 1 \end{cases}$$

**Surjection:** Let $y \in \mathbb{R}$. If $y \geq 0$, then we set $y = \dfrac{1}{x} - 2$. This gives $\dfrac{1}{x} = y + 2$ and $x = \dfrac{1}{y+2}$. Now $0 < x \leq \dfrac{1}{2}$. We have $f(x) = y + 2 - 2 = y$. If $y < 0$, then we set $y = \dfrac{1}{x-1} + 2$. We have $\dfrac{1}{x-1} = y - 2$ and $x = \dfrac{1}{y-2} + 1 = \dfrac{y-1}{y-2}$. Now $\dfrac{1}{2} < x < 1$ and $f(x) = y$.

**Injection**: Let us first note that if $0 < x \leq \dfrac{1}{2}$, then $f(x)$ is positive and if $\dfrac{1}{2} < x < 1$, then $f(x)$ is negative. This means that if $f(x) = f(y)$, we have only two possibilities:

(i) $0 < x, y \leq \dfrac{1}{2}$: If $f(x) = f(y)$, then $\dfrac{1}{x} - 2 = \dfrac{1}{y} - 2$, which is equivalent to $x = y$.

(ii) $\dfrac{1}{2} < x, y < 1$: If $f(x) = f(y)$, then $\dfrac{1}{x-1} + 2 = \dfrac{1}{y-1} + 2$ gives $x = y$.

Because $f$ is bijective, $|(0,1)| = |\mathbb{R}|$.

**6.** We prove that the are injections $f\colon (0,1) \times (0,1) \to (0,1)$ and $g\colon (0,1) \to (0,1) \to (0,1) \times (0,1)$.
(Injection $f$): Let $a \in (0,1)$. Then the map $f(x) = (a, x)$ is an injection $(0,1) \to (0,1) \times (0,1)$. Suppose that we have selected to represent real numbers so that the tail-end consists of 9's is excluded. Let

$$x = (0.a_1a_2a_3a_4a_5\cdots, 0.b_1b_2b_3b_4b_5\cdots) \in (0,1) \times (0,1).$$

(Injection $g$): Let us define $g(x)$ so that it is a number formed by taking decimal from the first 'coordinate' and 'second coordinate' one-by-one, that is,

$$g(x) = 0.a_1b_1a_2b_2a_3b_3a_4b_4a_5b_5\cdots$$

Now clearly $g(x) \in (0,1)$. The map $g$ is an injection, because if

$$f(x) = 0.a_1b_1a_2b_2a_3b_3a_4b_4a_5b_5\cdots$$
$$f(y) = 0.c_1d_1c_2d_2c_3d_3c_4d_4c_5d_5\cdots$$

then $a_i = c_i$ and $b_i = d_i$ for all $i \geq 0$. We obtain

$$x = (0.a_1a_2a_3a_4a_5\cdots, 0.b_1b_2b_3b_4b_5\cdots)$$
$$y = (0.c_1c_2c_3c_4c_5\cdots, 0.d_1d_2d_3d_4d_5\cdots)$$

We have that $f\colon (0,1) \times (0,1) \to (0,1)$ and $g\colon (0,1) \times (0,1) \to (0,1)$ are injections. By **Schröder–Bernstein theorem**, $|(0,1) \times (0,1)| = |(0,1)|$.
Because $\mathbb{C} = |\mathbb{R} \times \mathbb{R}| = |(0,1) \times (0,1)| = |(0,1)| = |\mathbb{R}|$, the claim is proved.

**1.**

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= (n-1)!\left(\frac{1}{k!(n-k-1)!} + \frac{1}{(k-1)!(n-k)!}\right) \\ &= (n-1)!\left(\frac{n-k}{k!(n-k)!} + \frac{k}{k!(n-k)!}\right) \\ &= (n-1)!\frac{n}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} \\ &= \binom{n}{k}.\end{aligned}$$

**2.** $(\forall n \geq 1)\, 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$

**Base** $n = 1$: Left side $1^2 = 1$, right side $\frac{1}{6} \cdot 1 \cdot 2 \cdot 3$

**Induction step:** Suppose that the claim holds for $n = k$, that is,

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

Let $n = k + 1$. Now

$$\begin{aligned}1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{1}{6}k(k+1)(2k+1) + \frac{6}{6}(k+1)^2 \\ &= \frac{1}{6}(k+1)[k(2k+1) + 6(k+1)] \\ &= \frac{1}{6}(k+1)[2k^2 + k + 6k + 6)] \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3) \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)\end{aligned}$$

that is, the claim holds for $n = k + 1$.

**3.** $(\forall n \geq 2)\, \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n}$

**Base** $n = 2$: Left side $\frac{1}{1 \cdot 2} = \frac{1}{2}$, right side $\frac{1}{2}$.

**Induction step:** Suppose that the claim holds for $n = k$, that is,

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k-1) \cdot k} = \frac{k-1}{k}$$

Let $n = k + 1$. Now

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k-1) \cdot k} + \frac{1}{k \cdot (k+1)} =$$

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

Thus, the claim holds also for $n = k + 1$.

**4.** $(\forall n \geq 2)\, \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 1$

Let $n \geq 2$. Because $n - 1 < n$, we have $(n-1)n < n \cdot n = n^2$ and

$$\frac{1}{n^2} < \frac{1}{n(n-1)}$$

We obtain

$$\frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n}$$

The last equality follows from Exercise 3. Because $n - 1 < n$, dividing by $n$ gives

$$\frac{n-1}{n} < 1,$$

which completes the proof.

**5.** $(\forall \geq 1)\, (1+x)^n \geq 1 + nx$, where $x \geq -1$

Note first that $x \geq -1$ is essential. If $x = -50$ and $n = 3$, then $(1-50)^3 = -117649$ and $1 - 3 \cdot 50 = -149$, and the claim does not hold. Because $1 + x \geq 0$, we can multiply numbers by it and the order of $\geq$-sign does not change in (**).

**Base** $n = 1$: Left side $(1+x)^1 = 1 + x$, right side $1 + 1 \cdot x = 1 + x$.

**Induction step:** Suppose that the claim holds for $n = k$, that is,

$$(1+x)^k \geq 1 + kx$$

Let $n = k + 1$.

$$\begin{aligned}(1+x)^{k+1} &= (1+x)^k(1+x) \overset{(**)}{\geq} (1+kx)(1+x) = 1 + x + kx + kx^2 \\ &= 1 + x(k+1) + kx^2 \geq 1 + (k+1)x,\end{aligned}$$

since $kx^2 \geq 0$. We have shown that the claim is true also for $k = n + 1$.

**6.** $(\forall n \geq 0)\, F_0 + F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

**Base** $n = 0$: Left side $F_0 = 0$, right side $F_2 - 1 = 1 - 1 = 0$.

**Induction step:** Suppose that the claim holds for $n = k$, that is,

$$F_0 + F_1 + F_2 + \cdots + F_k = F_{k+2} - 1.$$

Let $n = k + 1$. Now

$$\begin{aligned}F_0 + F_1 + F_2 + \cdots + F_k + F_{k+1} &= (F_{k+2} - 1) + F_{k+1} - 1 \\ &= F_{k+1} + F_{k+2} = F_{k+3} - 1 = F_{(k+1)+2} - 1.\end{aligned}$$

**1.** An integer $k$ with $n = ak$:

(a) $20 = 4 \cdot 5$
(b) $-25 = 5 \cdot (-5)$
(c) $9 = -3 \cdot -3$
(d) $-27 = -9 \cdot 3$
(e) $23 = 1 \cdot 23$
(f) $17 = -1 \cdot (-17)$
(g) $0 = -5 \cdot 0$
(h) $75 = 75 \cdot 1$

**2.** $a|b$ if there is $k$ such that $b = a \cdot k$.

(a) $x|0$, because $0 = x \cdot 0$
(b) $1|x$, because $x = 1 \cdot x$
(c) $x|x$, because $x = x \cdot 1$

**3.** We have that

$$\frac{2n+3}{n} = 2 + \frac{3}{n}.$$

The result is an integer if and only if $\frac{3}{n}$ is an integer. This happens exactly when $n \in \{-3, -1, 1, 3\}$.

(b) By definition $a \in \langle b \rangle \iff b|a$.
($\Rightarrow$) Suppose that $m|n$. If $a \in \langle n \rangle$, then $n|a$. We have by Lemma 1(b) that $m|a$. This means that $a \in \langle m \rangle$. We have proved $\langle n \rangle \subseteq \langle m \rangle$
($\Leftarrow$) Suppose $\langle n \rangle \subseteq \langle m \rangle$. Because $n \in \langle n \rangle \subseteq \langle m \rangle$, we have $m|n$.

**4.** We have that $\gcd(2016, 323) = 1$, because

$$\begin{aligned} 2016 &= 6 * 323 + 78 \\ 323 &= 4 * 78 + 11 \\ 78 &= 7 * 11 + 1 \\ 11 &= 11 * 1 + 0 \end{aligned}$$

We can now write

$$\begin{aligned} 1 = 78 - 7 * 11 = (2016 - 6 * 323) - 7 * (323 - 4 * 78) \\ = 2016 - 13 * 323 + 28 * 78 = 2016 - 13 * 323 + 28 * (2016 - 6 * 323) \\ = 29 * 2016 - (13 + 28 * 6) * 323 = \boxed{29} * 2016 - \boxed{181} * 323 \end{aligned}$$

**5.** (a) $\text{lcm}(8,12) = 24$, $\text{lcm}(20,30) = 60$, $\text{lcm}(51,68) = 204$, $\text{lcm}(23,18) = 414$

(b) For instance, $\gcd(51,68) = 17$ and $\text{lcm}(51,68) = 204$.
Now $51 * 68 = 3468$ and $17 * 204 = 3468$. It seems to be that

$$a * b = \text{lcm}(a,b) * \gcd(a,b)$$

(c) By (b), we have that

$$\text{lcm}(a,b) = \frac{a * b}{\gcd(a,b)}$$

We have $\gcd(301337, 307829) = 541$, because

$$\begin{aligned}
301337 &= 0 * 307829 + 301337 \\
307829 &= 1 * 301337 + 6492 \\
301337 &= 46 * 6492 + 2705 \\
6492 &= 2 * 2705 + 1082 \\
2705 &= 2 * 1082 + 541 \\
1082 &= 2 * 541 + 0
\end{aligned}$$

We can now solve

$$\text{lcm}(301337, 307829) = (301337 * 307829)/541 = 171\,460\,753$$

**6.** First we see that

$$\frac{ab}{\gcd(a,b)} = a\frac{b}{\gcd(a,b)} = b\frac{a}{\gcd(a,b)}$$

This means that $\dfrac{ab}{\gcd(a,b)}$ is a common multiple of $a$ and $b$. Because $\text{lcm}(a,b)$ is the smallest common multiple of $a$ and $b$, we have

$$\frac{ab}{\gcd(a,b)} \geq \text{lcm}(a,b) \tag{1}$$

On the other hand, by Theorem 2 (Division Theorem), we can write

$$ab = q\,\text{lcm}(a,b) + r, \text{ where } 0 \leq r < \text{lcm}(a,b).$$

Because $\text{lcm}(a,b) = sa$ and $\text{lcm}(a,b) = tb$ for some $s$ and $t$, we have $ab = qsa + r$. If we divide by $a$, we get $b = qs + \frac{r}{a}$. Similarly, we have $ab = qtb + r$ and dividing by $b$ we obtain $a = qt + \frac{r}{b}$. Suppose that $r \neq 0$. Then the above mean that $a|r$ and $b|r$. Therefore, there are $k_1$ and $k_2$ such that $r = k_1 a = k_2 b$, and $r$ is a common multiplier of $a$ and $b$. On the other hand $r < \text{lcm}(a,b)$, which contradicts the minimality of $\text{lcm}(a,b)$. Hence, we must have $r = 0$ and $\text{lcm}(a,b)$ divides $ab$. Notice that

$$\frac{ab}{\text{lcm}(a,b)} = \frac{a}{\text{lcm}(a,b)/b} = \frac{b}{\text{lcm}(a,b)/a}$$

is a common divisor of $a$ and $b$. By the maximality of the $\gcd(a, b)$,

$$\frac{ab}{\operatorname{lcm}(a, b)} \leq \gcd(a, b),$$

which directly gives

$$\frac{ab}{\gcd(a, b)} \leq \operatorname{lcm}(a, b) \tag{2}$$

Combining (1) and (2), we get

$$ab = \operatorname{lcm}(a, b) \gcd(a, b)$$

**1.** We get the last digit of $7^{150}$ by finding its remainder when divided by 10:

$$7^{150} \equiv (7^2)^{75} \equiv 49^{75} \equiv (-1)^{75} = -1 \equiv 9 \bmod 10.$$

This means that the last digit is 9.

**2.** We can select $x = 13$. Then $6x - 3 = 6 \cdot 13 - 3 = 78 - 3 = 75$. The following numbers are congruent with 75 modulo 17:

$$7 \equiv 24 \equiv 41 \equiv 58 \equiv 75 \equiv 92 \equiv \cdots$$

**3.** Let us denote the first three selected numbers by $s_1$, $s_2$, $s_3$. By the Division Theorem:

$$\begin{aligned} s_1 &= k_1 \cdot 3 + r_1, \\ s_2 &= k_2 \cdot 3 + r_2, \\ s_3 &= k_3 \cdot 3 + r_3, \end{aligned}$$

where $0 \leq r_1, r_2, r_3 < 3$. This gives that

$$s_1 + s_2 + s_3 = (k_1 + k_2 + k_3)3 + (r_1 + r_2 + r_3)$$

The only way that $s_1 + s_2 + s_3$ is divisible by 3 is when $r_1 + r_2 + r_3$ is divisible by 3. We have the following remainders:

$$\begin{aligned} 71 &\equiv 2 \bmod 3 \\ 76 &\equiv 1 \bmod 3 \\ 80 &\equiv 2 \bmod 3 \\ 82 &\equiv 1 \bmod 3 \\ 91 &\equiv 1 \bmod 3 \end{aligned}$$

This means that we must select 76, 82, 91. Note that 76 + 82 is divisible by 2, so we can select the first 3 digits in this order.

The sum $76 + 82 + 91$ is odd, but after adding the fourth number, the sum must be even – because it must be divisible by 4. This means that next we must insert 71. Note that the sum

$$76 + 82 + 91 + 71 = 320$$

is divisible by 4. The **last** number to insert is 80.

**4.** We have that

$$6! = 2^4 \cdot 3^2 \cdot 5,$$

which means that $6! \equiv 0 \bmod 9$. This implies that $k! \equiv 0 \bmod 9$ for all $6 \leq k \leq 999$. Now

$$\begin{aligned} 1! &= 1 \\ 2! &= 2 \\ 3! &= 6 \\ 4! &= 24 \equiv 6 \bmod 9 \\ 5! &\equiv 5 \cdot 6 = 30 \equiv 3 \bmod 9 \end{aligned}$$

The remainder of

$$1! + 2! + 3! + 4! + 5! + 6! + \cdots + 999!$$

divided by 9 is 0, because

$$1 + 2 + 6 + 6 + 3 = 18 \equiv 0 \bmod 9.$$

**5.** Clock works "modulo 24" with respect to hours. The plane arrives to Peking at

$$18{:}10 + 8{:}30 = 26{:}40 \equiv 2{:}40 \bmod 24h$$

Stockholm time. Because Peking time is 7 hours ahead Stockholm time, the time in Peking is

$$2{:}40 + \ 7 \text{ hours } = 9{:}40.$$

**6.** Let $a$, $b$ and $c > 0$ be integers such that $a \equiv b \bmod c$. This means that there are $s$, $t$, and $0 \leq r < n$ such that

$$a = sc + r \qquad \text{and} \qquad b = tc + r.$$

Then

$$a^2 = (sc + r)^2 = s^2c^2 + 2scr + r^2 = c(s^2c + 2sr) + r^2.$$

Similarly,

$$b^2 = (tc + r)^2 = t^2c^2 + 2tcr + r^2 = c(t^2c + 2tr) + r^2.$$

This means that $a^2 \equiv b^2 \bmod c$. By repeating this, we have that $a^n \equiv b^n \bmod c$ for all $n \geq 1$.

Because $2 \equiv 9 \bmod 7$, we have $2^n \equiv 9^n \bmod 7$. This implies that

$$2^n + 6 \cdot 9^n \equiv 9^n + 6 \cdot 9^n \equiv 7 \cdot 9^n \equiv 0 \bmod 7.$$

**1.**

```
THIS IS A VERY SECRET MESSAGE
GCRF RF K BZJQ FZOJZG AZFFKHZ
```

**2.** a) The number of letters in words is not the same; b) Secret message `OXAO` contains two `O`'s, but in `JOHN` all letters are different.

**3.** There was a hint which said that "The three most frequently occurring letters in the above text agree with the graph in Figure 1 of lecture notes." The three most frequent letters in the text are: `Z` (19 times), `C` (16 times), and `U` (12 times). In Figure 1, we see that the three most frequent letters in English are `E`, `T`, `A`. Therefore, we get `Z` $\leftrightarrow$ `E`, `C` $\leftrightarrow$ `T` and `U` $\leftrightarrow$ `A`.

If we look at the text, there are two different one-letter words. The other we only know, and it should be clear what the other is. After we replace the known letters, we see that there are several instances of the `T?E` and `T?`. In this way, one can proceed. The message is

```
L A S T   N I G H T   I   D R E A M T   I
W E N T   T O   M A N D E R L E Y   A G A I N.
I T   S E E M E D   T O   M E   I   S T O O D
B Y   T H E   I R O N   G A T E S   L E A D I N G
T O   T H E   D R I V E   A N D   F O R   A
W H I L E   I   C O U L D   N O T   E N T E R
T H E   W A Y   W A S   B A R R E D
T O   M E.
```

**4.** An easy way is to write a short Python script:

```
for n in range(2, 982340323):
    if 982340323 % n == 0:
        print(n)
```

It prints the numbers:

```
1459
673297
```

**5.** a) $n = 109 \cdot 131 = 14279$ and $\phi = (109 - 1) \cdot (131 - 1) = 14279 = 14040$.

b) Let us select $e = 12473$. Now $\gcd(14040, 12473) = 1$:

$$\begin{aligned}
14040 &= 1 * 12473 + 1567 \\
12473 &= 7 * 1567 + 1504 \\
1567 &= 1 * 1504 + 63 \\
1504 &= 23 * 63 + 55 \\
63 &= 1 * 55 + 8 \\
55 &= 6 * 8 + 7 \\
8 &= 1 * 7 + 1 \\
7 &= 7 * 1 + 0
\end{aligned}$$

c) $C = \text{rem}(9876^{12473}, 14279)$. We can compute this using Python:

```
>>> pow(9876, 12473, 14279)
8431
```

**6.** a) We have

$$\begin{aligned}
1 &= 8 - 7 = (63 - 55) - (55 - 6 * 8) = 63 - 2 * 55 + 6 * (63 - 55) = 7 * 63 - 8 * 55 \\
&= 7 * (1567 - 1504) - 8 * (1504 - 23 * 63) \\
&= 7 * 1567 - 15 * 1504 - 8 * (-23 * (1567 - 1504)) \\
&= (7 + 8 * 23) * 1567 + (-15 - 8 * 23) * 1504 = 191 * 1567 - 199 * 1504 \\
&= 191 * (14040 - 12473) - 199 * (12473 - 7 * 1567) \\
&= 191 * (14040 - 12473) - 199 * (12473 - 7 * (14040 - 12473)) \\
&= (191 + 199 * 7) * 14040 - (191 + 199 + 199 * 7) * 12473 \\
&= 1584 * 14040 - 1783 * 12473
\end{aligned}$$

The multiplicative inverse of 12473 is $-1783 \equiv 12257 \bmod \phi$.
b) Using Python we have:

```
>>> pow(8431, 12257, 14279)
9876
```

We managed to get back the original message!

**1.**

$$A+B=\begin{bmatrix}4&0\\4&4\\2&6\end{bmatrix} \quad \text{and} \quad A-B=\begin{bmatrix}2&-4\\0&-2\\4&2\end{bmatrix}$$

**2.** (a)

$$A^{\mathrm{T}}=\begin{bmatrix}-3&0&-1&2\\1&-3&1&-2\end{bmatrix} \quad \text{and} \quad b^{\mathrm{T}}=\begin{bmatrix}1&-1\\-2&2\\2&0\\3&4\end{bmatrix}$$

(b)

$$AB=\begin{bmatrix}-4&8&-6&-5\\3&-6&0&-12\\-2&4&-2&1\\4&-8&4&-2\end{bmatrix}$$

**3.** For

$$\begin{bmatrix}a&b\\c&d\end{bmatrix}$$

the inverse is

$$\frac{1}{(ad-bc)}\begin{bmatrix}d&-b\\-c&a\end{bmatrix}.$$

Now $ad-bc=7\cdot 18-10\cdot 11=16$. This gives that

$$A^{-1}=\begin{bmatrix}18/16&10/16\\11/16&7/16\end{bmatrix}=\begin{bmatrix}9/8&5/8\\11/16&7/16\end{bmatrix}$$

**4.** Consider the product

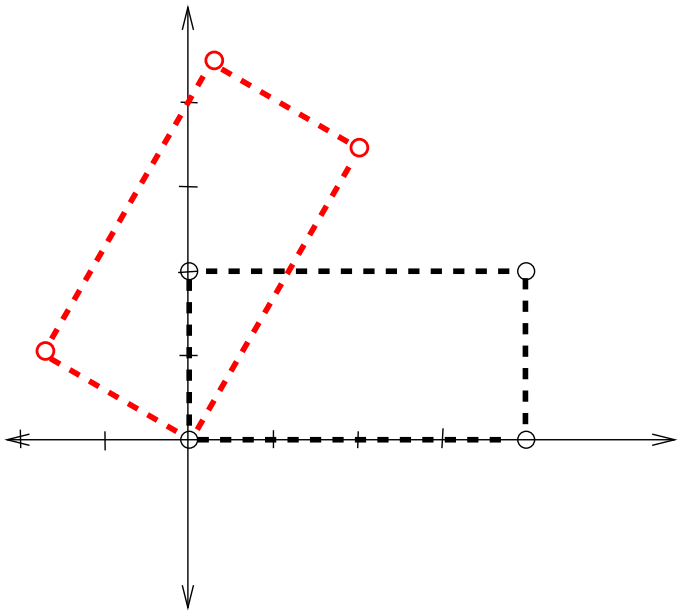
$$\begin{bmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x\cos\theta-y\sin\theta\\x\sin\theta+y\cos\theta\end{bmatrix}$$

Because $\theta=60°$, $\cos\theta=1/2$ and $\sin\theta=\sqrt{3}/2\approx 0.866$. Therefore, this is what happens to one point:

$$(x,y)\mapsto(0.5x-0.866y,0.866x+0.5y).$$

This means that

$$\begin{aligned}&(0,0)\mapsto(0,0)\\&(0,2)\mapsto(0.5\cdot 0-0.866\cdot 2,0.866\cdot 0+0.5\cdot 2)=(-1.732,1)\\&(4,0)\mapsto(0.5\cdot 4-0.866\cdot 0,0.866\cdot 4+0.5\cdot 0)=(2,3.464)\\&(4,2)\mapsto(0.5\cdot 4-0.866\cdot 2,0.866\cdot 4+0.5\cdot 2)=(0.268,4.464)\end{aligned}$$



**1.** Let $A$ be the following augmented matrix

$$\left[\begin{array}{rrr|r} 4 & -1 & 3 & 5 \\ 0 & 2 & 5 & 9 \\ -6 & 1 & -3 & 10 \end{array}\right] \underset{\text{(a)}}{\Rightarrow} \left[\begin{array}{rrr|r} 20 & -5 & 15 & 25 \\ 0 & 2 & 5 & 9 \\ -6 & 1 & -3 & 10 \end{array}\right]$$

$$\left[\begin{array}{rrr|r} 4 & -1 & 3 & 5 \\ 0 & 2 & 5 & 9 \\ -6 & 1 & -3 & 10 \end{array}\right] \underset{\text{(b)}}{\Rightarrow} \left[\begin{array}{rrr|r} 4 & -1 & 3 & 5 \\ -6 & 1 & -3 & 10 \\ 0 & 2 & 5 & 9 \end{array}\right]$$

$$\left[\begin{array}{rrr|r} 4 & -1 & 3 & 5 \\ 0 & 2 & 5 & 9 \\ -6 & 1 & -3 & 10 \end{array}\right] \underset{\text{(b)}}{\Rightarrow} \left[\begin{array}{rrr|r} 4 & -1 & 3 & 5 \\ 12 & -1 & 14 & 24 \\ -6 & 1 & -3 & 10 \end{array}\right]$$

**2.** The biggest difficulty in this exercise is that one needs to be **very** careful in details. Let $A = (a_{ij})_{m\times n}$ and $B = (b_{ij})_{n\times p}$. We set $AB = (c_{ij})_{m\times p}$. Therefore,

$$c_{ij} = a_{i1}\cdot b_{1j} + a_{i2}\cdot b_{2j} + \cdots + a_{in}\cdot b_{nj}$$

and

$$c_{ji} = a_{j1}\cdot b_{1i} + a_{j2}\cdot b_{2i} + \cdots + a_{jn}\cdot b_{ni}$$

Let $(d_{ij})_{p\times m} = (AB)^{\mathrm{T}}$. We have that $d_{ij} = c_{ji}$. On the other hand, let

$$B^{\mathrm{T}} = (e_{ij})_{p\times n}, \quad A^{\mathrm{T}} = (f_{ij})_{n\times m}, \quad B^{\mathrm{T}}A^{\mathrm{T}} = (g_{ij})_{p\times n}.$$

This means that $e_{ij} = b_{ji}$ and $f_{ij} = a_{ji}$. Now

$$\begin{aligned} g_{ij} &= e_{i1}\cdot f_{1j} + e_{i2}\cdot f_{2j} + \cdots e_{in}\cdot f_{nj} \\ &= b_{1i}\cdot a_{j1} + b_{2i}\cdot a_{j2} + \cdots b_{ni}\cdot a_{jn} \\ &= a_{j1}\cdot b_{1i} + a_{j2}\cdot b_{2i} + \cdots + a_{jn}\cdot b_{ni}. \end{aligned}$$

We have that $d_{ij} = g_{ij}$. Thus, $(AB)^{\mathrm{T}} = B^{\mathrm{T}}A^{\mathrm{T}}$.

**3.** For

$$A = \begin{bmatrix} 10 & 0 & -3 \\ -2 & -4 & 1 \\ 3 & 0 & 2 \end{bmatrix},$$

$$\det A = 10\cdot \det\begin{bmatrix} -4 & 1 \\ 0 & 2 \end{bmatrix} - 0\cdot \det\begin{bmatrix} -2 & 1 \\ 3 & 2 \end{bmatrix} + c\cdot \det\begin{bmatrix} -2 & -4 \\ 3 & 0 \end{bmatrix}$$

Because $b = 0$, we do not need to compute the determinant of the "middle" case. We have

$$\det\begin{bmatrix} -4 & 1 \\ 0 & 2 \end{bmatrix} = -4\cdot -0 = -8 \quad \text{and} \quad \det\begin{bmatrix} -2 & -4 \\ 3 & 0 \end{bmatrix} = 0 - 3\cdot(-4) = 12$$

Thus, $\det A = 10\cdot(-8) - 0 + (-3)\cdot 12 = -80 - 36 = -116$.

**4.** There are several paths which lead to the unique reduced row echelon form. This is one possibility:

$$\begin{bmatrix} 7 & -8 & -12 \\ -4 & 2 & 3 \end{bmatrix} \overset{2R_2+R_1\to R_2}{\Rightarrow} \begin{bmatrix} -1 & -4 & -6 \\ -4 & 2 & 3 \end{bmatrix} \overset{-1R_1\to R_1}{\Rightarrow} \begin{bmatrix} 1 & 4 & 6 \\ -4 & 2 & 3 \end{bmatrix} \overset{4R_1+R_2\to R_2}{\Rightarrow}$$

$$\begin{bmatrix} 1 & 4 & 6 \\ 0 & 18 & 27 \end{bmatrix} \overset{\frac{1}{18}R_2\to R_2}{\Rightarrow} \begin{bmatrix} 1 & 4 & 6 \\ 0 & 1 & \frac{3}{2} \end{bmatrix} \overset{-4R_2+R_1\to R_1}{\Rightarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \frac{3}{2} \end{bmatrix}$$

This gives the solution $x = 0$ and $y = \frac{3}{2}$.

**5.** We reduce $A$ to $I_3$:

$$\begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ 2 & 3 & -4 \end{bmatrix} \overset{-R_1+R_2\to R_2}{\Rightarrow} \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 2 & 3 & -4 \end{bmatrix} \overset{-2R_1+R_3\to R_3}{\Rightarrow} \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 5 & -4 \end{bmatrix} \overset{-5R_2+R_3\to R_3}{\Rightarrow} \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\overset{R_3+R_2\to R_2}{\Rightarrow} \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \overset{R_2+R_1\to R_1}{\Rightarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We get $A^{-1}$ by applying the above operations to $I_3$ in the same order:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \overset{-R_1+R_2\to R_2}{\Rightarrow} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \overset{-2R_1+R_3\to R_3}{\Rightarrow} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix} \overset{-5R_2+R_3\to R_3}{\Rightarrow} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 3 & -5 & 1 \end{bmatrix}$$

$$\overset{R_3+R_2\to R_2}{\Rightarrow} \begin{bmatrix} 1 & 0 & 0 \\ 2 & -4 & 1 \\ 3 & -5 & 1 \end{bmatrix} \overset{R_2+R_1\to R_1}{\Rightarrow} \begin{bmatrix} 3 & -4 & 1 \\ 2 & -4 & 1 \\ 3 & -5 & 1 \end{bmatrix}$$

The result can be verified by multiplying:

$$\begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ 2 & 3 & -4 \end{bmatrix} \begin{bmatrix} 3 & -4 & 1 \\ 2 & -4 & 1 \\ 3 & -5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

By Proposition 18 this is enough to show that these two matrices are inverses.

**6.** (a)

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \text{and} \quad M_S = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

(b) $M_{R\circ S} = M_R \circ M_S$:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

(c) Let us first form $M_{R^{-1}} = (M_R)^{\mathrm{T}}$

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Now the matrix of $R \circ R^{-1}$ can be formed as the product

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$