CSCA67 - Assignment #3

Satyajit Datta 1012033336

November 21, 2025

1. Proof Strategies

1.1

We write a | b, read "a divides b", to stand for $\exists k, b = ak$. Prove that if 4 divides $a - b$, then it also divides $a^2 - b^2$.

Proof

$$
\begin{array}{lr}
\text{Suppose } 4 \mid (a+b) & (1) \\
\quad \exists k, a+b = 4k & \text{1, Def of } x \mid y \ \ (2) \\
\quad a+b = 4k & \text{2, E.I} \ \ (3) \\
\quad a^2 - b^2 = (a+b)(a-b) & (4) \\
\qquad\qquad = 4k(a-b) & \text{Math} \qquad \\
\quad \exists k, a^2 - b^2 = 4k & \text{4, E.G} \ \ (5) \\
\quad 4 \mid \left(a^2 - b^2\right) & \text{5, Def of } x \mid y \ \ (6) \\
4 \mid (a+b) \rightarrow 4 \mid \left(a^2 + b^2\right) & \text{1, 6, Implication} \ \ (7)
\end{array}
$$

As required to prove. ■.

1.2

For all real numbers x and y, $\min(x, y) = (x + y - |x - y|)/2$ and $\max(x, y) = (x + y + |x - y|)/2$

WTS: $\forall x, y, \min(x, y) = (x + y - |x - y|)/2$

Let x, y be arbitrary.		(1)
Assume $x \le y$		(2)
$\min(x, y) = x$	2	(3)
$x - y \le 0$	2	(4)
$\lvert x - y \rvert = -(x - y)$	4, def^n of $\lvert \cdot \rvert$	(5)
$(x + y - \lvert x - y \rvert)/2 = (x + y - (-(x - y)))/2$	5	(6)
$= (x - y - (-x + y))/2$		
$= 2x/2$		
$= x$		
$\min(x, y) = (x + y - \lvert x - y \rvert)/2$	3, 6	(7)
$x \le y \to (\min(x, y) = (x + y - \lvert x - y \rvert)/2)$	2, 7, implication	(8)
Assume $x \ge y$		(9)
$\min(x, y) = y$	9	(10)
$x - y \ge 0$	9	(11)
$\lvert x - y \rvert = x - y$	11, def^n of $\lvert \cdot \rvert$	(12)
$(x + y - \lvert x - y \rvert)/2 = (x + y - (x - y))/2$	12	(13)
$= (x - y - x + y)/2$		
$= 2y/2$		
$= y$		
$\min(x, y) = (x + y - \lvert x - y \rvert)/2$	10, 13	(14)
$x \ge y \to (\min(x, y) = (x + y - \lvert x - y \rvert)/2)$	9, 14, implication	(15)
$\min(x, y) = (x + y - \lvert x - y \rvert)/2$	8, 15, Cases	(16)
$\forall x, y, \min(x, y) = (x + y - \lvert x - y \rvert)/2$	$1, 16, U.G$	(17)

As required to show. ■.

WTS: $\max(x, y) = (x + y + \lvert x - y \rvert)/2$

Let x, y be arbitrary.		(1)
Assume $x \le y$		(2)
$\max(x,y) = y$	2	(3)
$x - y \le 0$	2	(4)
$\mid x - y \mid = -(x-y)$	4, def^n of $\mid \cdot \mid$	(5)
$(x+y+\mid x-y \mid)/2 = (x+y+(-(x-y)))/2$	5	(6)
$= (x-y+(-x+y))/2$		
$= 2y/2$		
$= y$		
$\max(x,y) = (x+y+\mid x-y \mid)/2$	3, 6	(7)
$x \le y \to (\max(x,y) = (x+y+\mid x-y \mid)/2)$	2, 7, implication	(8)
Assume $x \ge y$		(9)
$\max(x,y) = x$	9	(10)
$x - y \ge 0$	9	(11)
$\mid x - y \mid = x - y$	11, def^n of $\mid \cdot \mid$	(12)
$(x+y+\mid x-y \mid)/2 = (x+y+(x-y))/2$	12	(13)
$= 2x/2$		
$= x$		
$\max(x,y) = (x+y+\mid x-y \mid)/2$	10, 13	(14)
$x \ge y \to (\max(x,y) = (x+y+\mid x-y \mid)/2)$	9, 14, implication	(15)
$\max(x,y) = (x+y+\mid x-y \mid)/2$	8, 15, Cases	(16)
$\forall x, y, \max(x,y) = (x+y+\mid x-y \mid)/2$	$1, 16, U.G$	(17)

As required to show. ■.

1.3

Recall that x is irrational if there are no integers a and b, such that $x = \frac{a}{b}$. Prove that the third power of any real number is irrational only if the number itself is irrational.

WTS: $x^3 \notin \mathbb{Q} \to x \notin \mathbb{Q}$

Proof.

$$
\begin{array}{llr}
\text{Suppose } x \in \mathbb{Q} & & (1)\\
\quad \exists a,b \in \mathbb{Z}\left(x = \frac{a}{b}\right) \wedge (b \neq 0) & 1, \text{Def}^n \text{ of } \mathbb{Q} & (2)\\
\quad \left(x = \frac{a}{b}\right) \wedge (b \neq 0) & 2, \text{E.I} & (3)\\
\quad x = \frac{a}{b} & 3, \text{simp.} & (4)\\
\quad b \neq 0 & 3, \text{simp.} & (5)\\
\quad x^3 = \frac{a^3}{b^3} & 4, \text{math} & (6)\\
\quad c = a^3 & 2, 6 & (7)\\
\quad d = b^3 & 2, 6 & (8)\\
\quad d \neq 0 & 7, 5 & (9)\\
\quad x^3 = \frac{c}{d} & 6, 7, 8 & (10)\\
\quad \left(x^3 = \frac{c}{d}\right) \wedge (d \neq 0) & 9, 10, \text{conj.} & (11)\\
\quad \exists a,b \in \mathbb{Z}, \left(x^3 = \frac{a}{b}\right) \wedge (b \neq 0) & 11, \text{E.G} & (12)\\
\quad x^3 \in \mathbb{Q} & 12, \text{Def}^n \text{ of } \mathbb{Q} & (13)\\
x \in \mathbb{Q} \rightarrow x^3 \in \mathbb{Q} & 1, 13, \text{imp.} & (14)\\
x^3 \notin \mathbb{Q} \rightarrow x \notin \mathbb{Q} & 14, \text{contr.} & (15)
\end{array}
$$

As required to show. ■.

1.4

Prove that if x is rational, then $x+\sqrt{2}$ is not. You may use the fact that $\sqrt{2}$ is irrational, as we proved in class.

$$
\begin{array}{lr}
\text{Suppose } x \in \mathbb{Q} & (1) \\
\quad \text{Suppose } x+\sqrt{2} \in \mathbb{Q} & \text{For contradiction} \quad (2) \\
\quad\quad \exists a,b \in \mathbb{Z}, \left(x = \frac{a}{b}\right) \wedge (b \neq 0) & 1, \text{Def}^n \text{ of } \mathbb{Q} \quad (3) \\
\quad\quad \exists a,b \in \mathbb{Z}, \left(x+\sqrt{2} = \frac{a}{b}\right) \wedge (b \neq 0) & 2, \text{Def}^n \text{ of } \mathbb{Q} \quad (4) \\
\quad\quad \left(x = \frac{a}{b}\right) \wedge (b \neq 0) & 3, \text{E.I} \quad (5) \\
\quad\quad \left(x+\sqrt{2} = \frac{c}{d}\right) \wedge (d \neq 0) & 4, \text{E.I} \quad (6) \\
\quad\quad x = \frac{a}{b} & 5, \text{simp.} \quad (7) \\
\quad\quad x+\sqrt{2} = \frac{c}{d} & 6, \text{simp.} \quad (8) \\
\quad\quad b \neq 0 & 5, \text{simp} \quad (9) \\
\quad\quad d \neq 0 & 6, \text{simp} \quad (10) \\
\quad\quad x+\sqrt{2}-x = \frac{a}{b} - \frac{c}{d} & 7, 8 \quad (11) \\
\quad\quad\quad\quad\quad\quad = \frac{ad-bc}{bd} & \\
\quad\quad \sqrt{2} = \frac{ad-bc}{bd} & 11, \text{math} \quad (12) \\
\quad\quad bd \neq 0 & 9, 10 \quad (13) \\
\quad\quad \left(\sqrt{2} = \frac{ad-bc}{bd}\right) \wedge (bd \neq 0) & 12, 13, \text{conj.} \quad (14) \\
\quad\quad \exists f,g \in \mathbb{Z}, \left(\sqrt{x} = \frac{f}{g}\right) \wedge (g \neq 0) & 14, \text{E.G} \quad (15) \\
\quad\quad \sqrt{2} \in \mathbb{Q} & 15, \text{Def}^n \text{ of } \mathbb{Q} \quad (16) \\
\quad\quad \text{A contradiction} & (17) \\
\quad x+\sqrt{2} \notin \mathbb{Q} & 2, 16, \text{contradiction} \quad (18) \\
x \in \mathbb{Q} \rightarrow x+\sqrt{2} \notin \mathbb{Q} & 1, 17, \text{imp.} \quad (19)
\end{array}
$$

As required to show. ■.

1.5

Using the same definition of rational as above, prove or disprove: If x is irrational, then so is $x+\sqrt{2}$

We will disprove this statement.
Let $x = -\sqrt{2}$
Therefore, x is irrational.
$x+\sqrt{2} = -\sqrt{2}+\sqrt{2} = 0$
0 is rational.

Therefore, we have shown a counterexample where the hypothesis is true and the conclusion is false, therefore this statement is not valid.

2. Induction

2.1

Prove that:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

for all positive integers n.

Base Case.

$$\sum_{i=1}^{n} i^2 = 1$$
$$\frac{(1)(1+1)(2+1)}{6} = 1$$

Therefore, P(1)
Let $P(n)$ be $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.
WTS: $\forall k \geq 0, P(k) \rightarrow P(k+1)$

Let k be arbitrary (1)
Suppose $k \geq 1$ (2)
Suppose P(k) Induction Hypothesis (3)

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6} \quad \text{3, Def}^n \text{ of P (4)}$$

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 \quad \text{math (5)}$$
$$= \frac{k(k+1)(2k+1)}{6} + (n+1)^2 \quad \text{IH}$$
$$= \frac{k(k+1)(2k+1)}{6} +$$
$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6}$$
$$= \frac{(k+1)(k(2k+1) + 6(k+1))}{6}$$
$$= \frac{(k+1)\left(2k^2 + k + 6k + 6\right)}{6}$$
$$= \frac{(k+1)\left(2k^2 + 7k + 6\right)}{6}$$
$$= \frac{(k+1)(k+3)(2k+3)}{6}$$
$$= \frac{(k+1)(k+2)(2k+3)}{6}$$
$$= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$$

$P(k+1)$ 5, Def^n of P (6)
$P(k) \rightarrow P(k+1)$ 3, 6, implication (7)
$k \geq 1 \rightarrow (P(k) \rightarrow P(k+1))$ 2, 7, implication (8)
$\forall k \geq 1, P(k) \rightarrow P(k+1)$ 1, 8, U.G (9)

Therefore, $\forall n \geq 1, P(n)$, as required to show. ■.

2.2

Prove that

$$n! > 2^n$$

for all $n \geq 4$

Base Case.

$$4! = 24$$
$$2^4 = 16$$

Therefore, P(4)
Let $P(n)$ be $n! > 2^n$.
WTS: $\forall k \geq 4, P(k) \rightarrow P(k+1)$

Let k be arbitrary	(1)
Suppose $k \geq 4$	(2)
Suppose P(k)	Induction Hypothesis (3)
$(k+1)! = k! \cdot (k+1)$	Math (4)
$< 2^n \cdot (k+1)$	IH
$< 2^n \cdot 2$	$2 \leq 4 \leq k$
$= 2^{n+1}$	
$P(k+1)$	4, Def^n of P (5)
$P(k) \rightarrow P(k+1)$	3, 5, implication (6)
$k \geq 4 \rightarrow (P(k) \rightarrow P(k+1))$	2, 6, implication (7)
$\forall k \geq 4, P(k) \rightarrow P(k+1)$	1, 7, U.G (8)

Therefore, $\forall n \geq 4, P(n)$, as required to show. ■.

2.3

Prove that $3^{2n} - 1$ is divisible by 8, for all positive integers n.

Base Case.

$$3^2 - 1 = 8$$
$$8 \mid 8$$

Therefore, P(1)
Let $P(n)$ be $\exists k, 3^{2n} - 1 = 8k$.
WTS: $\forall k \geq 0, P(k) \rightarrow P(k+1)$

Let k be arbitrary		(1)
Suppose $k \geq 1$		(2)
Suppose P(k)	Induction Hypothesis	(3)
$\exists m, 3^{2k} - 1 = 8m$	3, Def^n of P	(4)
$3^{2k} - 1 = 8m$	4, E.I	(5)
$3^{2(k+1)} - 1 = 3^{2k+2} - 1$	math	(6)
$= (9)3^{2k} - 1$		
$= (8+1)3^{2k} - 1$		
$= 8\left(3^{2k}\right) + 3^{2k} - 1$		
$= 8\left(3^{2k}\right) + 3^{2k} - 1$		
$= 8\left(3^{2k}\right) + 8m$	5, IH	
$= 8\left(3^{2k} + m\right)$		
$\exists m, 3^{2(k+1)} - 1 = 8m$	6, E.G	(7)
$P(k+1)$	7, Def^n of P	(8)
$P(k) \rightarrow P(k+1)$	3, 8, implication	(9)
$k \geq 1 \rightarrow (P(k) \rightarrow P(k+1))$	2, 9, implication	(10)
$\forall k \geq 1, P(k) \rightarrow P(k+1)$	1, 10, U.G	(11)

Therefore, $\forall n \geq 1, P(n)$, as required to show. ■.

2.4

Prove that

$$\sum_{j=1}^{n} \frac{j}{(j+1)!} \leq 1 - \frac{1}{(n+1)!}$$

for all $n \geq 1$.

Base Case.

$$\sum_{j=1}^{1} \frac{j}{(j+1)!} = \frac{1}{2}$$

$$1 - \frac{1}{(1+1)!} = \frac{1}{2}$$

Therefore, P(1)
Let $P(n)$ be $\sum_{j=1}^{n} \frac{j}{(j+1)!} \leq 1 - \frac{1}{(n+1)!}$.
WTS: $\forall k \geq 0, P(k) \rightarrow P(k+1)$

Let k be arbitrary (1)

Suppose $k \geq 1$ (2)

Suppose P(k) Induction Hypothesis (3)

$$
\begin{aligned}
\sum_{j=1}^{k+1} \frac{j}{(j+1)!} &= \sum_{j=1}^{k} \frac{j}{(j+1)!} + \frac{k+1}{(k+2)!} && (4)\\
&\leq 1 - \frac{1}{(k+1)!} + \frac{k+1}{(k+2)!} && \text{IH}\\
&= 1 - \left(\frac{1}{(k+1)!} - \frac{k+1}{(k+2)!}\right)\\
&= 1 - \left(\frac{k+2}{(k+1)!(k+2)} - \frac{k+1}{(k+2)!}\right)\\
&= 1 - \left(\frac{k+2}{(k+2)!} - \frac{k+1}{(k+2)!}\right)\\
&= 1 - \frac{k+2-(k+1)}{(k+2)!}\\
&= 1 - \frac{1}{(k+2)!}\\
&= 1 - \frac{1}{((k+1)+1)!}
\end{aligned}
$$

$P(k+1)$ 4, Def^n of P (5)

$P(k) \to P(k+1)$ 3, 5, implication (6)

$k \geq 1 \to (P(k) \to P(k+1))$ 2, 6, implication (7)

$\forall k \geq 1, P(k) \to P(k+1)$ 1, 7, U.G (8)

Therefore, $\forall n \geq 1, P(n)$, as required to show. ■.

3.5

Prove that if $A_1, A_2, \ldots A_n$ and B are sets, then

$$(A_1\ B) \cup (A_2\ B) \cup \ldots \cup (A_n\ B) = (A_1 \cup A_2 \cup \ldots \cup A_n)\ B$$

for all $n \geq 2$

Base Case.

$$
\begin{aligned}
(A_1\ B) \cup (A_2\ B) &= x : (x \in A_1 \wedge x \notin B) \vee (x \in A_2 \wedge x \notin B)\\
&= x : (x \notin B) \wedge (x \in A_1 \vee x \in A_2)\\
&= (A_1 \cup A_2)\ B
\end{aligned}
$$

Therefore, P(2)
Let $P(n)$ be $(A_1\ B) \cup (A_2\ B) \cup \ldots \cup (A_n\ B) = (A_1 \cup A_2 \cup \ldots \cup A_n)\ B$.
WTS: $\forall k \geq 2, P(k) \to P(k+1)$

Let k be arbitrary (1)

Suppose $k \geq 2$ (2)

Suppose P(k) Induction Hypothesis (3)

$$(A_1 \; B) \cup (A_2 \; B) \cup \ldots \cup (A_{k+1} \; B) = (A_1 \; B) \cup (A_2 \; B) \cup \ldots \cup (A_k \; B) \cup (A_{k+1} \; B) \quad (4)$$

$$= (A_1 \cup A_2 \cup \ldots \cup A_k) \cup (A_{k+1} \; B) \quad \text{IH}$$

$$= x : (x \notin B \wedge (x \in A_1 \vee x \in A_2 \vee \ldots \vee A_k)) \vee (x \notin B \wedge x \in A_{k+1})$$

$$= x : (x \notin B) \wedge (x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_{k+1})$$

$$= (A_1 \cup A_2 \cup \ldots \cup A_{k+1}) \; B$$

$P(k+1)$ 4, Def^n of P (5)

$P(k) \rightarrow P(k+1)$ 3, 5, implication (6)

$k \geq 2 \rightarrow (P(k) \rightarrow P(k+1))$ 2, 6, implication (7)

$\forall k \geq 2, P(k) \rightarrow P(k+1)$ 1, 7, U.G (8)

3. Quantifier and Logical Implication and Equivalence

3.1

$$(\forall x, P(x)) \rightarrow (\exists x, Q(x)) \text{ and } \exists x, P(x) \rightarrow Q(x)$$

$(\forall x, P(x)) \rightarrow (\exists x, Q(x))$ (1)

$\neg(\forall x, P(x)) \vee (\exists x, Q(x))$ cond. (2)

$\exists x, \neg P(x) \vee \exists x, Q(x)$ q.neg (3)

$\exists x, (\neg P(x) \vee Q(x))$ distr. (4)

$\exists x, (P(x) \rightarrow Q(x))$ cond. (5)

Therefore, $A \rightarrow B$ and $B \rightarrow A$ are both tautologies, since the statements are logically equivalent.

3.2

$$\exists x \forall y, P(x, y) \text{ and } \forall y \exists x, P(x, y)$$

$\exists x \forall y, P(x, y)$ (1)

$\forall y, P(a, y)$ 1, E.I (2)

Let y be arbitrary (3)

$P(a, y)$ 2, 3, U.I (4)

$\exists x, P(x, y)$ 4, E.G (5)

$\forall y, \exists x, P(x, y)$ 3, 5, U.G (6)

Thus, $A \to B$ is a tautology.
However, let $W \subseteq U = \emptyset$
For A, since there are no elements in W, the statement can never be true.
For B, since there are no elements in W, the statement is vacuously true.
Thus, we have shown a statement where $B \to A$ is not a tautology.

3.3

Assuming a non-empty universe of discourse, $\exists x \forall y, P(x) \to Q(y)$ and $(\forall y, Q(y)) \vee (\exists x, \neg P(x))$.

$\exists x \forall y, P(x) \to Q(y)$		(1)
$\forall y, P(a) \to Q(y)$	1, E.I	(2)
Let y be arbitrary		(3)
$P(a) \to Q(y)$	2, 3, U.I	(4)
$\neg P(a) \vee Q(y)$	4, cond.	(5)
$(\forall y, Q(y)) \vee \neg P(a)$	5, 3, U.G	(6)
$(\forall y, Q(y)) \vee (\exists x, \neg P(x))$	7, E.G	(7)

Therefore, $A \to B$ is a tautology.

$(\forall y, Q(y)) \vee (\exists x, \neg P(x))$	$(\forall y, Q(y)) \vee \neg P(a)$1, E.I	(1)
Let y be arbitrary		(2)
$Q(y) \vee \neg P(a)$	2, 3 U.I	(3)
$P(a) \to Q(y)$	4, cond.	(4)
$\forall y, P(a) \to Q(y)$	3, 5, U.G	(5)
$\exists x, \forall y, P(x) \to Q(y)$		(6)

Therefore, $B \to A$ is a tautology.

3.4

Assuming a non-empty universe of discourse, $\exists x \forall y, P(y) \to Q(x)$ and $(\forall y, P(y)) \to (\exists x, Q(x))$.

Assume $\exists x \forall y, P(y) \to Q(x)$		(1)
$\forall y, P(y) \to Q(a)$	1, E.I	(2)
Let y be arbitrary		(3)
Assume P(y)		(4)
$Q(a)$	4, 2, M.P	(5)
$\exists x Q(x)$	5, E.G	(6)
$P(y) \to \exists x, Q(x)$	4, 6, implication	(7)
$(\forall y, P(y)) \to (\exists x, Q(x))$	2, 7, U.G	(8)
$\exists x \forall y, P(y) \to Q(x) \to (\forall y, Q(y)) \to (\exists x, P(x))$		(9)

Thus, $A \to B$ is a tautology.
Let $W \subseteq U = a, b$, where $P(a) = T, Q(b) = False, P(b) = False, Q(b) = False$
A:

$$
\begin{aligned}
\exists x \forall y, P(y) \rightarrow Q(x) \\
((P(a) \rightarrow Q(a)) \vee (P(a) \rightarrow Q(b))) \wedge ((P(b) \rightarrow Q(a)) \vee (P(b) \rightarrow Q(b))) \\
((T \rightarrow F) \vee (T \rightarrow F)) \wedge ((F \rightarrow F) \vee (F \rightarrow F)) \\
((F \vee F) \wedge (T \vee T)) \\
F \wedge T \\
F
\end{aligned}
$$

$$
\begin{aligned}
(\forall y, P(y)) \rightarrow (\exists x, Q(x)) \\
(P(a) \wedge P(b)) \rightarrow (Q(a) \vee Q(b)) \\
(T \wedge F) \rightarrow (F \vee F) \\
F \rightarrow F \\
T
\end{aligned}
$$

Thus, $B \rightarrow A$ is not a tautology.
$\exists a, b, (n = ab) \wedge (0 < a < n) \wedge (0 < b < n)$

$$dotted \tag{1}$$