HSC Math Extension 2: The Nature of Proof

Vu Hung Nguyen

1 Introduction

1.1 Project Overview

This booklet presents a comprehensive collection of proof problems for HSC Mathematics Extension 2 students. The 30 carefully selected problems cover all essential proof techniques: Direct Proof, Proof by Contradiction, Mathematical Induction, and Proof by Cases. Topics include divisibility, irrationality, modular arithmetic, parity, and logical reasoning.

The collection is divided into two parts:

- **Part 1 (15 problems):** Detailed step-by-step solutions showing complete reasoning, algebraic manipulation, and justification of each step. Each solution is designed to fit within one page, modeling clear and concise proof writing.
- **Part 2 (15 problems):** Strategic hints and solution sketches using flipped hint environments, encouraging independent problem-solving while providing guidance on key steps.

1.2 Target Audience

This booklet is designed for HSC Mathematics Extension 2 students who want to:

- Master fundamental proof techniques required for the HSC examination
- Develop rigorous mathematical reasoning and proof-writing skills
- Build confidence with both standard and non-standard proof problems
- Understand connections between different proof methods
- Practice problems at Easy, Medium, and Hard difficulty levels

Teachers and tutors will also find this collection valuable for:

- Demonstrating worked examples with clear pedagogical progression
- Selecting problems at appropriate difficulty levels for students
- Providing comprehensive coverage of HSC Extension 2 proof topics
- Preparing students for examination standards in mathematical proof

1.3 How to Use This Booklet

For Students:

- Begin with the Proof Primer below to review fundamental concepts and techniques.
- Work through Part 1 problems first, attempting each problem before reading the detailed solution.
- Compare your proof structure and reasoning with the provided solutions.
- Pay attention to the "Takeaways" section after each solution—these highlight key techniques and common pitfalls.
- Move to Part 2 problems, using the upside-down hints only after making a genuine attempt.
- Revisit challenging problems after a few days to reinforce understanding and technique.

For Tutors and Teachers:

- Use Part 1 problems as worked examples in lessons, highlighting proof structure and key techniques.
- Assign Part 2 problems for homework or practice, encouraging students to attempt problems before revealing hints.
- Select problems by proof technique or topic to target specific areas of the syllabus.
- Use the variety of difficulty levels (Easy, Medium, Hard) to differentiate instruction for different student abilities.
- Note Problem 14 (Part 1) as the "Induction Crossover" demonstrating overlap with HSC-Induction collection.

1.4 Proof Primer

Essential Number Theory Concepts

1. Divisibility: $a|b$ (read "a divides b") means there exists an integer k such that $b = ak$.

2. Division Algorithm: For integers a and $b > 0$, there exist unique integers q (quotient) and r (remainder) such that:

$$a = bq + r, \quad 0 \leq r < b$$

This is essential for case-based proofs (e.g., classifying integers as $3k$, $3k + 1$, or $3k + 2$).

3. Modular Arithmetic: $a \equiv b \pmod{m}$ (read "a is congruent to b modulo m") means $m|(a - b)$. Equivalently, a and b have the same remainder when divided by m.

Key Properties:

- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for any positive integer n

4. Parity: An integer is *even* if it can be written as $2k$ for some integer k. An integer is *odd* if it can be written as $2k + 1$ for some integer k.

5. Prime Numbers: An integer $p > 1$ is prime if its only positive divisors are 1 and p. Key property: If prime p divides ab, then $p|a$ or $p|b$.

Essential Proof Techniques

1. Direct Proof: Start with given information and use logical steps to reach the desired conclusion.

- Example: To prove $a|b$ and $b|c$ implies $a|c$, write $b = ak_1$ and $c = bk_2$, then $c = (ak_1)k_2 = a(k_1k_2)$.

2. Proof by Contradiction (Reductio ad Absurdum):

- Assume the negation of what you want to prove
- Use logical reasoning to derive a statement that contradicts a known fact, the hypothesis, or a mathematical truth
- Conclude that the assumption must be false, hence the original statement is true
- Example: Proving $\sqrt{2}$ is irrational by assuming $\sqrt{2} = \frac{p}{q}$ and deriving a contradiction

3. Mathematical Induction: To prove $P(n)$ is true for all integers $n \geq n_0$:

- *Base Case:* Prove $P(n_0)$ is true
- *Inductive Hypothesis:* Assume $P(k)$ is true for some arbitrary $k \geq n_0$
- *Inductive Step:* Prove $P(k+1)$ is true using the assumption that $P(k)$ is true
- *Conclusion:* By the principle of mathematical induction, $P(n)$ is true for all $n \geq n_0$

4. Proof by Cases: When the hypothesis can be divided into distinct cases:

- Identify all possible cases (ensure they are exhaustive and mutually exclusive)
- Prove the statement for each case separately
- Conclude that the statement holds in all cases
- Example: Proving $n^2 \equiv 0$ or $1 \pmod 4$ by checking cases n even and n odd

5. Biconditional Proof (If and Only If): To prove "P if and only if Q" (written $P \iff Q$):

- Prove the forward direction: $P \implies Q$
- Prove the reverse direction: $Q \implies P$
- Both directions must be proven independently

6. Inequality Proofs: Common strategies for proving inequalities:

- *Algebraic manipulation:* Transform the inequality to an obviously true statement (show $A \geq B$ by proving $A - B \geq 0$)
- *AM-GM Inequality:* For non-negative numbers: $\frac{a_1+\cdots+a_n}{n} \geq \sqrt[n]{a_1 \cdots a_n}$
- *Cauchy-Schwarz:* $(a_1b_1 + \cdots + a_nb_n)^2 \leq (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2)$
- *Induction:* For inequalities involving n, establish base case and inductive step

Induction Variants

Beyond the standard induction framework, several specialized variants frequently appear:

Induction for Series: Proving closed-form formulas for sums (e.g., $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$). In the inductive step, add the $(k+1)$-th term to both sides of $P(k)$ and simplify algebraically.

Induction for Divisibility: Proving statements like "$n|f(n)$ for all $n \geq n_0$". Use the inductive hypothesis to express $f(k+1)$ in terms of $f(k)$ and factor to show divisibility.

Induction for Inequalities: Proving statements like "$2^n > n^2$ for $n \geq 5$". The inductive step requires showing $f(k+1) > g(k+1)$ using the assumption $f(k) > g(k)$, often with careful estimation.

Induction for Recursive Sequences: For recursively defined sequences $a_{n+1} = f(a_n)$, prove properties by expressing a_{k+1} using the recurrence and applying the inductive hypothesis to a_k.

Strong Induction: Assume $P(n_0), P(n_0+1), \ldots, P(k)$ all true, then prove $P(k+1)$. Essential when the $(k+1)$-th case depends on multiple previous cases.

Common Proof Strategies

Contrapositive: To prove $P \implies Q$, instead prove $\neg Q \implies \neg P$ (logically equivalent).

Consecutive Integers: Among k consecutive integers, exactly one is divisible by k. Among 2 consecutive integers, exactly one is even.

Irrationality Proofs: Standard template for proving $\sqrt{n}$ irrational (where n is not a perfect square):

1. Assume $\sqrt{n} = \frac{p}{q}$ in lowest terms ($\gcd(p,q) = 1$)
2. Square both sides: $n = \frac{p^2}{q^2}$, so $p^2 = nq^2$
3. Show $n|p^2$ implies $n|p$ (using prime factorization if n is prime)
4. Substitute $p = nk$, derive $q^2 = nk^2$, showing $n|q$
5. Contradict $\gcd(p,q) = 1$

2 Part 1: Problems with Detailed Solutions

Easy Problems (5 problems)

Problem 2.1: Easy

Prove by contradiction that $\sqrt{3} + \sqrt{5} > \sqrt{11}$.

Solution 2.1

Proof by Contradiction

Step 1: Assume the negation

Assume, for the sake of contradiction, that the statement is false. That is, assume:

$$\sqrt{3} + \sqrt{5} \leq \sqrt{11}$$

Step 2: Square both sides

Since all terms are positive, we can square both sides without changing the inequality:

$$\begin{aligned}(\sqrt{3} + \sqrt{5})^2 &\leq (\sqrt{11})^2 \\ 3 + 2\sqrt{3} \cdot \sqrt{5} + 5 &\leq 11 \\ 8 + 2\sqrt{15} &\leq 11 \\ 2\sqrt{15} &\leq 3\end{aligned}$$

Step 3: Square again

Both sides are still positive, so square again:

$$\begin{aligned}(2\sqrt{15})^2 &\leq 3^2 \\ 4 \cdot 15 &\leq 9 \\ 60 &\leq 9\end{aligned}$$

Step 4: Establish contradiction

The statement $60 \leq 9$ is clearly false.

This contradiction arose from our assumption that $\sqrt{3} + \sqrt{5} \leq \sqrt{11}$.

Therefore, our assumption must be false, and we conclude:

$$\sqrt{3} + \sqrt{5} > \sqrt{11}$$

□

Takeaways 2.1

- **Proof by Contradiction Structure:** Assume the negation of what you want to prove, derive a logical impossibility, conclude original statement must be true
- **Squaring Inequalities:** When both sides are positive, squaring preserves the inequality direction
- **Algebraic Manipulation:** Expand $(\sqrt{3}+\sqrt{5})^2$ carefully: $(a+b)^2 = a^2+2ab+b^2$
- **Clear Contradictions:** A numerical impossibility like $60 \leq 9$ is an immediate and decisive contradiction

Problem 2.2: Easy

Show that there are no positive integers x and y such that $x^2 - y^2 = 1$.

Solution 2.2

Proof by Factorization and Case Analysis

Step 1: Factor the left side

We factor $x^2 - y^2$ as a difference of squares:

$$x^2 - y^2 = (x - y)(x + y) = 1$$

Step 2: Analyze integer factor pairs

Since x and y are positive integers, both $(x - y)$ and $(x + y)$ are integers. We need their product to equal 1.

The only ways to write 1 as a product of integers are:

- $1 = 1 \times 1$
- $1 = (-1) \times (-1)$

Step 3: Case 1 - Both factors equal 1

If $x - y = 1$ and $x + y = 1$, adding these equations gives:

$$2x = 2 \implies x = 1$$

Subtracting: $2y = 0 \implies y = 0$

But $y = 0$ contradicts the requirement that y is a positive integer.

Step 4: Case 2 - Both factors equal -1

If $x - y = -1$ and $x + y = -1$, adding these equations gives:

$$2x = -2 \implies x = -1$$

But $x = -1$ contradicts the requirement that x is a positive integer.

Conclusion

All possible integer factorizations of 1 lead to violations of the positive integer requirement.

Therefore, there are no positive integers x and y satisfying $x^2 - y^2 = 1$.

□

Takeaways 2.2

- **Factorization Strategy:** Recognize $x^2 - y^2 = (x - y)(x + y)$ as difference of squares
- **Integer Factor Analysis:** For product $(x - y)(x + y) = 1$, only factor pairs are $(1, 1)$ and $(-1, -1)$
- **Systematic Case Checking:** Solve simultaneous equations $x-y = a$ and $x+y = b$ for each factor pair (a, b)
- **Constraint Verification:** Always check solutions against domain restrictions (here: positive integers)

Problem 2.3: Easy

Prove that $\sqrt{23}$ is irrational.

Solution 2.3

Proof by Contradiction

Step 1: Assume the negation

Assume, for contradiction, that $\sqrt{23}$ is rational. Then it can be written as:

$$\sqrt{23} = \frac{p}{q}$$

where $p, q \in \mathbb{Z}$, $q \neq 0$, and $\gcd(p, q) = 1$ (the fraction is in lowest terms).

Step 2: Square both sides

$$23 = \frac{p^2}{q^2}$$
$$p^2 = 23q^2$$

Step 3: Deduce divisibility

From $p^2 = 23q^2$, we see that p^2 is divisible by 23.

Since 23 is prime, if $23 \mid p^2$, then $23 \mid p$ (by fundamental theorem of arithmetic).

Step 4: Substitute and derive contradiction

Since $23 \mid p$, write $p = 23k$ for some integer k. Substituting into $p^2 = 23q^2$:

$$(23k)^2 = 23q^2$$
$$529k^2 = 23q^2$$
$$23k^2 = q^2$$

This shows q^2 is divisible by 23. Since 23 is prime, $23 \mid q$.

Step 5: Establish contradiction

We have shown that both p and q are divisible by 23.

This contradicts our assumption that $\gcd(p, q) = 1$.

Conclusion

Therefore, $\sqrt{23}$ cannot be expressed as a fraction of integers.

Hence, $\sqrt{23}$ is irrational.

□

Takeaways 2.3

- **Standard Irrationality Template:** Assume rational form $\frac{p}{q}$ in lowest terms, square to get $p^2 = nq^2$, show both p and q divisible by prime factor, contradict lowest terms assumption
- **Prime Divisibility:** If prime p divides a^2, then p divides a (key property from fundamental theorem of arithmetic)
- **Lowest Terms:** Always start with $\gcd(p, q) = 1$ to enable the contradiction via common factors
- **Generalization:** This method proves $\sqrt{p}$ irrational for any prime p

Problem 2.4: Easy

Consider the statement: "For all integers n, if n is a multiple of 6, then n is a multiple of 2."
Which of the following is the contrapositive of this statement?

A. There exists an integer n such that n is a multiple of 6 and not a multiple of 2.

B. There exists an integer n such that n is a multiple of 2 and not a multiple of 6.

C. For all integers n, if n is not a multiple of 2, then n is not a multiple of 6.

D. For all integers n, if n is not a multiple of 6, then n is not a multiple of 2.

Solution 2.4

Logical Analysis of Contrapositive
Step 1: Identify the logical structure
The original statement has the form:

$$\forall n \in \mathbb{Z}, \quad P(n) \implies Q(n)$$

Where:

- $P(n)$: "n is a multiple of 6"
- $Q(n)$: "n is a multiple of 2"

Step 2: Apply contrapositive definition
The contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$.
Key: The universal quantifier ("for all") remains unchanged.
Step 3: Negate each part

- $\neg Q(n)$: "n is NOT a multiple of 2"
- $\neg P(n)$: "n is NOT a multiple of 6"

Step 4: Construct the contrapositive

$$\forall n \in \mathbb{Z}, \quad \neg Q(n) \implies \neg P(n)$$

In words: "For all integers n, if n is not a multiple of 2, then n is not a multiple of 6."
This matches **Option C**.
Analysis of incorrect options:

- **Option A:** Negation of original ($\exists n : P(n) \wedge \neg Q(n)$), not contrapositive
- **Option B:** Negation of converse
- **Option D:** Inverse ($\neg P \implies \neg Q$), not contrapositive

Answer: $\boxed{\text{C}}$

Takeaways 2.4

- **Contrapositive Form:** $P \implies Q$ has contrapositive $\neg Q \implies \neg P$ (swap and negate both parts)
- **Logical Equivalence:** A statement and its contrapositive are logically equivalent (same truth value)
- **Quantifiers Unchanged:** Universal quantifier ("for all") stays when forming contrapositive
- **Common Errors:** Inverse ($\neg P \implies \neg Q$) and converse ($Q \implies P$) are NOT equivalent to original

Problem 2.5: Easy

Prove that $n^2 - 1$ is divisible by 3 if n is not a multiple of 3.

Solution 2.5

Proof by Cases (Modular Arithmetic)
Step 1: Set up the cases
If n is not a multiple of 3, then $n \not\equiv 0 \pmod 3$.
By the division algorithm, n must satisfy one of:

- $n \equiv 1 \pmod 3$, or
- $n \equiv 2 \pmod 3$

We will prove $n^2 - 1 \equiv 0 \pmod 3$ in both cases.
Step 2: Case 1 - $n \equiv 1 \pmod 3$

$$\begin{aligned} n^2 - 1 &\equiv (1)^2 - 1 \pmod 3 \\ &\equiv 1 - 1 \pmod 3 \\ &\equiv 0 \pmod 3 \end{aligned}$$

Therefore, $3 \mid (n^2 - 1)$ in this case.
Step 3: Case 2 - $n \equiv 2 \pmod 3$

$$\begin{aligned} n^2 - 1 &\equiv (2)^2 - 1 \pmod 3 \\ &\equiv 4 - 1 \pmod 3 \\ &\equiv 3 \pmod 3 \\ &\equiv 0 \pmod 3 \end{aligned}$$

Therefore, $3 \mid (n^2 - 1)$ in this case as well.
Conclusion
Since $n^2 - 1 \equiv 0 \pmod 3$ in all possible cases where $3 \nmid n$, we conclude that $n^2 - 1$ is divisible by 3 whenever n is not a multiple of 3.

□

Takeaways 2.5

- **Proof by Cases Setup:** If $n \not\equiv 0 \pmod{m}$, check all other residue classes modulo m
- **Modular Arithmetic:** Use $a \equiv b \pmod{m}$ to mean $m \mid (a - b)$, or equivalently, a and b have same remainder when divided by m
- **Complete Case Coverage:** For modulo 3, only residues are 0, 1, 2; excluding 0 leaves exactly 2 cases to check
- **Calculation Technique:** Substitute residue values directly: if $n \equiv 2 \pmod{3}$, then $n^2 \equiv 4 \equiv 1 \pmod{3}$

Medium Problems (5 problems)

Problem 2.6: Medium

Prove that if a is any odd integer, then $a^2 - 1$ is divisible by 8.

Solution 2.6

Direct Proof

Step 1: Express a as an odd integer

Since a is odd, we can write:

$$a = 2k + 1$$

for some integer k.

Step 2: Expand $a^2 - 1$

$$\begin{aligned} a^2 - 1 &= (2k+1)^2 - 1 \\ &= 4k^2 + 4k + 1 - 1 \\ &= 4k^2 + 4k \\ &= 4k(k+1) \end{aligned}$$

Step 3: Analyze $k(k+1)$

Note that k and $(k+1)$ are consecutive integers.

Therefore, one of them must be even, which means their product $k(k+1)$ is divisible by 2.

Write $k(k+1) = 2m$ for some integer m.

Step 4: Substitute and conclude

$$\begin{aligned} a^2 - 1 &= 4 \cdot k(k+1) \\ &= 4 \cdot 2m \\ &= 8m \end{aligned}$$

Since $a^2 - 1 = 8m$, we conclude that $a^2 - 1$ is divisible by 8.

□

Takeaways 2.6

- **Odd Integer Form:** Any odd integer can be written as $2k + 1$ for some integer k
- **Consecutive Integer Property:** Product of consecutive integers $k(k + 1)$ is always even (one must be even)
- **Factor Extraction:** From $4k(k + 1) = 4 \cdot 2m = 8m$, directly see divisibility by 8
- **Alternative View:** Can also factor $a^2 - 1 = (a - 1)(a + 1)$, both even for odd a, with one divisible by 4

Problem 2.7: Medium

(a) Given a is integral and not divisible by 5, prove the remainder when a^2 is divided by 5 is either 1 or 4.

(b) Hence, given that a, b are integral and not divisible by 5, prove that $a^4 - b^4$ is divisible by 5.

Solution 2.7

Part (a): Proof by Cases

Since a is not divisible by 5, we have $a \not\equiv 0 \pmod 5$.
By the division algorithm, a must be congruent to 1, 2, 3, or 4 modulo 5.
We check each case:

Case 1: $a \equiv 1 \pmod 5$

$$a^2 \equiv 1^2 \equiv 1 \pmod 5$$

Case 2: $a \equiv 2 \pmod 5$

$$a^2 \equiv 2^2 \equiv 4 \pmod 5$$

Case 3: $a \equiv 3 \pmod 5$

$$a^2 \equiv 3^2 \equiv 9 \equiv 4 \pmod 5$$

Case 4: $a \equiv 4 \pmod 5$

$$a^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod 5$$

In all cases, $a^2 \equiv 1$ or $4 \pmod 5$.
Therefore, the remainder when a^2 is divided by 5 is either 1 or 4. □

Part (b): Using Part (a)

From part (a), for any integer x not divisible by 5: $x^2 \equiv 1$ or $4 \pmod 5$.
Consider $a^4 = (a^2)^2$:

- If $a^2 \equiv 1 \pmod 5$, then $(a^2)^2 \equiv 1^2 \equiv 1 \pmod 5$
- If $a^2 \equiv 4 \pmod 5$, then $(a^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod 5$

Thus $a^4 \equiv 1 \pmod 5$ for any integer a not divisible by 5.
Similarly, $b^4 \equiv 1 \pmod 5$.
Therefore:

$$\begin{aligned} a^4 - b^4 &\equiv 1 - 1 \pmod 5 \\ &\equiv 0 \pmod 5 \end{aligned}$$

Hence $5 \mid (a^4 - b^4)$. □

Takeaways 2.7

- **Systematic Case Analysis:** For $5 \nmid a$, check all residues $a \equiv 1, 2, 3, 4 \pmod 5$ systematically
- **Squaring Congruences:** If $a \equiv b \pmod m$, then $a^2 \equiv b^2 \pmod m$
- **"Hence" Strategy:** Part (b) builds directly on part (a)'s result; apply it twice to get $a^4 \equiv b^4 \equiv 1 \pmod 5$
- **Fermat's Little Theorem Preview:** Result $a^4 \equiv 1 \pmod 5$ for $\gcd(a, 5) = 1$ is special case of FLT

Problem 2.8: Medium

Prove by contradiction that if a, b are integers and $a + b \leq 5$, then $a \leq 2$ or $b \leq 2$.

Solution 2.8

Proof by Contradiction

Step 1: Assume the negation of the conclusion

We want to prove: If $a + b \leq 5$, then $a \leq 2$ or $b \leq 2$.

Assume the conclusion is false. The negation of "$a \leq 2$ or $b \leq 2$" is:

$$a > 2 \quad \text{AND} \quad b > 2$$

Step 2: Apply the integer constraint

Since a and b are integers with $a > 2$ and $b > 2$, we must have:

$$a \geq 3 \quad \text{and} \quad b \geq 3$$

(The smallest integer greater than 2 is 3.)

Step 3: Derive a contradiction

Adding these inequalities:

$$a + b \geq 3 + 3$$
$$a + b \geq 6$$

But this contradicts our hypothesis that $a + b \leq 5$.

We cannot have both $a + b \geq 6$ and $a + b \leq 5$ simultaneously.

Conclusion

Since assuming the negation of the conclusion leads to a contradiction, the conclusion must be true.

Therefore, if a, b are integers with $a + b \leq 5$, then $a \leq 2$ or $b \leq 2$.

□

Takeaways 2.8

- **Negating "Or" Statements:** The negation of "P or Q" is "not P AND not Q"
- **Integer Constraints:** For integers, $a > 2$ implies $a \geq 3$ (no integers strictly between 2 and 3)
- **Contradiction Structure:** Derive statement that directly contradicts a hypothesis (here: $a + b \geq 6$ vs $a + b \leq 5$)
- **Logical Form:** Statement has form $(P \implies Q \vee R)$; negate conclusion to get $\neg Q \wedge \neg R$

Problem 2.9: Medium

Prove that a number is divisible by 4 if and only if the last two digits form a number divisible by 4.

Solution 2.9

Biconditional Proof (If and Only If)
This requires proving both directions:
Forward Direction ($\implies$): If N is divisible by 4, then its last two digits form a number divisible by 4.
Reverse Direction ($\impliedby$): If the last two digits form a number divisible by 4, then N is divisible by 4.

Setup: Express any integer N as:

$$N = 100A + L$$

where A is the number formed by all digits except the last two, and L is the two-digit number formed by the last two digits ($0 \leq L \leq 99$).

Forward Direction Proof:
Assume $4 \mid N$, so $N \equiv 0 \pmod 4$.
Then:

$$100A + L \equiv 0 \pmod 4$$

Since $100 = 4 \times 25$, we have $100A \equiv 0 \pmod 4$.
Therefore:

$$\begin{aligned} 0 + L &\equiv 0 \pmod 4 \\ L &\equiv 0 \pmod 4 \end{aligned}$$

Thus $4 \mid L$. □

Reverse Direction Proof:
Assume $4 \mid L$, so $L \equiv 0 \pmod 4$.
Since $100 = 4 \times 25$, we have $100A \equiv 0 \pmod 4$.
Therefore:

$$\begin{aligned} N = 100A + L &\equiv 0 + 0 \pmod 4 \\ N &\equiv 0 \pmod 4 \end{aligned}$$

Thus $4 \mid N$. □

Conclusion:
Since both directions are proven, we conclude:

$$N \text{ is divisible by } 4 \iff \text{last two digits of } N \text{ divisible by } 4$$

Takeaways 2.9

- **Iff Proof Structure:** Must prove both ($\implies$) and ($\impliedby$) directions independently
- **Digit Representation:** Writing $N = 100A + L$ separates last two digits for modular analysis
- **Key Observation:** Since $100 \equiv 0 \pmod 4$, divisibility of N by 4 depends only on last two digits
- **Generalization:** Same technique proves divisibility rules for powers of 2 (e.g., rule for 8 uses last three digits)

Problem 2.10: Medium

Prove that if m, n are integers, then $m^2 - n^2$ is even if and only if at least one of $(m+n)$ and $(m-n)$ is even.

Solution 2.10

Biconditional Proof
Step 1: Factor the expression

$$m^2 - n^2 = (m-n)(m+n)$$

This factorization will be used in both directions.

Forward Direction ($\implies$): If $m^2 - n^2$ is even, then at least one of $(m+n)$ or $(m-n)$ is even.

Proof. Since $m^2 - n^2$ is even, the product $(m-n)(m+n)$ is even.
A product of two integers is even if and only if at least one factor is even.
Therefore, at least one of $(m-n)$ or $(m+n)$ must be even. □ □

Reverse Direction ($\impliedby$): If at least one of $(m+n)$ or $(m-n)$ is even, then $m^2 - n^2$ is even.

Proof. We consider two cases:
Case 1: $(m+n)$ is even.
Write $(m+n) = 2k$ for some integer k.
Then:

$$m^2 - n^2 = (m-n)(m+n) = (m-n)(2k) = 2k(m-n)$$

Since $k(m-n)$ is an integer, $m^2 - n^2$ is even.
Case 2: $(m-n)$ is even.
Write $(m-n) = 2j$ for some integer j.
Then:

$$m^2 - n^2 = (m-n)(m+n) = (2j)(m+n) = 2j(m+n)$$

Since $j(m+n)$ is an integer, $m^2 - n^2$ is even.
In both cases, $m^2 - n^2$ is even. □ □

Conclusion:
Both directions proven, therefore:

$$m^2 - n^2 \text{ is even} \iff \text{at least one of } (m+n), (m-n) \text{ is even}$$

Takeaways 2.10

- **Factorization First:** Factoring $m^2 - n^2 = (m-n)(m+n)$ immediately connects to parity of factors
- **Product Parity:** Product even $\iff$ at least one factor even (fundamental parity property)
- **Case Analysis:** Reverse direction handles two cases (either factor even) separately
- **Note on Parity:** Actually, $(m+n)$ and $(m-n)$ always have same parity (both even or both odd), so "at least one even" is equivalent to "both even"

Hard Problems (5 problems)

Problem 2.11: Hard

Explain why there is no integer n such that $(n+1)^{41} - 79n^{40} = 2$.

Solution 2.11

Proof by Modular Analysis and Case Checking
Step 1: Test $n = 0$
If $n = 0$:

$$(0+1)^{41} - 79(0)^{40} = 1 - 0 = 1 \neq 2$$

So $n = 0$ is not a solution.
Step 2: Analyze for $n \neq 0$ using modular arithmetic
For $n \neq 0$, consider the equation modulo n:
By the Binomial Theorem:

$$(n+1)^{41} = \sum_{k=0}^{41} \binom{41}{k} n^k \cdot 1^{41-k}$$

All terms contain n except the last term ($k = 0$):

$$(n+1)^{41} \equiv 1 \pmod{n}$$

The term $-79n^{40}$ is clearly divisible by n:

$$-79n^{40} \equiv 0 \pmod{n}$$

Therefore:

$$\begin{aligned} (n+1)^{41} - 79n^{40} &\equiv 2 \pmod{n} \\ 1 - 0 &\equiv 2 \pmod{n} \\ 1 &\equiv 2 \pmod{n} \end{aligned}$$

Step 3: Interpret the congruence
$1 \equiv 2 \pmod{n}$ means $n \mid (1-2)$, so $n \mid (-1)$.
Therefore $n \in \{-1, 1\}$.
Step 4: Test candidate values
For $n = 1$:

$$(1+1)^{41} - 79(1)^{40} = 2^{41} - 79 = 2,199,023,255,552 - 79 \neq 2$$

For $n = -1$:

$$(-1+1)^{41} - 79(-1)^{40} = 0 - 79(1) = -79 \neq 2$$

Conclusion
All possible integer values of n have been checked and none satisfy the equation.
Therefore, there is no integer n such that $(n+1)^{41} - 79n^{40} = 2$.

□

Takeaways 2.11

- **Modular Arithmetic Strategy:** Working mod n can dramatically constrain possible solutions
- **Binomial Expansion Mod n:** $(n+1)^k \equiv 1 \pmod{n}$ since all terms except constant contain n
- **Divisor Analysis:** $1 \equiv 2 \pmod{n}$ means $n \mid (-1)$, giving only $n \in \{-1, 1\}$
- **Exhaustive Checking:** After constraining to finitely many cases, verify each directly

Problem 2.12: Hard

The numbers a_n, for integers $n \geq 1$, are defined as:

$$a_1 = \sqrt{2}$$
$$a_2 = \sqrt{2 + \sqrt{2}}$$
$$a_3 = \sqrt{2 + \sqrt{2 + \sqrt{2}}}, \text{ and so on.}$$

These numbers satisfy the relation $a_{n+1}^2 = 2 + a_n$, for $n \geq 1$. (Do NOT prove this.)
Use mathematical induction to prove that $a_n = 2\cos\left(\frac{\pi}{2^{n+1}}\right)$ for all integers $n \geq 1$.

Solution 2.12

Proof by Mathematical Induction
Base Case $(n = 1)$:
LHS: $a_1 = \sqrt{2}$ (given)
RHS: $2\cos\left(\frac{\pi}{2^{1+1}}\right) = 2\cos\left(\frac{\pi}{4}\right) = 2 \cdot \frac{\sqrt{2}}{2} = \sqrt{2}$
Since LHS = RHS, the statement holds for $n = 1$. ✓

Inductive Hypothesis:
Assume the statement is true for $n = k$, where k is a positive integer:

$$a_k = 2\cos\left(\frac{\pi}{2^{k+1}}\right)$$

Inductive Step:
We must prove the statement for $n = k + 1$:

$$a_{k+1} = 2\cos\left(\frac{\pi}{2^{k+2}}\right)$$

Using the recurrence relation $a_{k+1}^2 = 2 + a_k$ and the inductive hypothesis:

$$\begin{aligned} a_{k+1}^2 &= 2 + 2\cos\left(\frac{\pi}{2^{k+1}}\right) \\ &= 2\left[1 + \cos\left(\frac{\pi}{2^{k+1}}\right)\right] \end{aligned}$$

Apply the double angle identity: $1 + \cos(2\theta) = 2\cos^2(\theta)$.
Let $2\theta = \frac{\pi}{2^{k+1}}$, so $\theta = \frac{\pi}{2^{k+2}}$:

$$\begin{aligned} a_{k+1}^2 &= 2 \cdot 2\cos^2\left(\frac{\pi}{2^{k+2}}\right) \\ &= 4\cos^2\left(\frac{\pi}{2^{k+2}}\right) \end{aligned}$$

Taking square roots:

$$a_{k+1} = \pm 2\cos\left(\frac{\pi}{2^{k+2}}\right)$$

Since $n \geq 1$, we have $0 < \frac{\pi}{2^{k+2}} < \frac{\pi}{2}$, so $\cos\left(\frac{\pi}{2^{k+2}}\right) > 0$.
Also, a_n is defined as nested square roots of positive numbers, so $a_{k+1} > 0$.
Therefore:

$$a_{k+1} = 2\cos\left(\frac{\pi}{2^{k+2}}\right)$$

This completes the inductive step. ✓

Conclusion:
By mathematical induction, $a_n = 2\cos\left(\frac{\pi}{2^{n+1}}\right)$ for all integers $n \geq 1$.

□

Takeaways 2.12

- **Induction with Recurrence:** Use given recurrence relation in inductive step to relate a_{k+1} to a_k
- **Double Angle Formula:** Identity $1 + \cos(2\theta) = 2\cos^2(\theta)$ is key to converting sum to square
- **Sign Consideration:** Must justify taking positive square root using domain/range analysis
- **Angle Halving:** Pattern shows a_n relates to cos of successively halved angles $(\pi/4, \pi/8, \pi/16, \ldots)$

Problem 2.13: Hard

Prove that for any integer $n > 1$, $\log_n(n+1)$ is irrational.

Solution 2.13

Proof by Contradiction

Step 1: Assume the negation

Assume, for contradiction, that $\log_n(n+1)$ is rational for some integer $n > 1$.
Then we can write:

$$\log_n(n+1) = \frac{p}{q}$$

where p, q are positive integers.

Step 2: Convert to exponential form

By definition of logarithm:

$$n^{p/q} = n + 1$$

Raising both sides to the power q:

$$n^p = (n+1)^q$$

Step 3: Analyze modulo n

Left side: $n^p \equiv 0 \pmod{n}$ (clearly divisible by n)
Right side: By the Binomial Theorem:

$$(n+1)^q = \sum_{k=0}^{q} \binom{q}{k} n^k \cdot 1^{q-k} = n^q + \binom{q}{1} n^{q-1} + \ldots + \binom{q}{q-1} n + 1$$

All terms contain n except the last term, so:

$$(n+1)^q \equiv 1 \pmod{n}$$

Step 4: Derive contradiction

From $n^p = (n+1)^q$, we have modulo n:

$$0 \equiv 1 \pmod{n}$$

This means $n \mid (0-1)$, so $n \mid (-1)$.
For $n > 1$, this is impossible.

Conclusion

The assumption that $\log_n(n+1)$ is rational leads to a contradiction.
Therefore, $\log_n(n+1)$ is irrational for all integers $n > 1$.

□

Takeaways 2.13

- **Logarithm to Exponential:** Converting $\log_n(n+1) = \frac{p}{q}$ to $n^p = (n+1)^q$ enables algebraic manipulation
- **Modular Analysis:** Working mod n reveals contradiction: LHS $\equiv 0$ but RHS $\equiv 1$
- **Binomial Expansion:** $(n+1)^q \equiv 1 \pmod{n}$ since only constant term survives
- **Non-standard Irrationality:** Unlike $\sqrt{p}$ proofs, this uses modular arithmetic rather than prime factorization

Problem 2.14: Hard

Prove by induction that $x^n - y^n$ is divisible by $x - y$ for all positive integers n, where x, y are integers with $x \neq y$.

Solution 2.14

Proof by Mathematical Induction
Base Case ($n = 1$):
For $n = 1$:

$$x^1 - y^1 = x - y$$

Since $x - y$ is divisible by $x - y$, the statement holds for $n = 1$. ✓

Inductive Hypothesis:
Assume the statement is true for $n = k$, where k is a positive integer:

$$x^k - y^k \text{ is divisible by } x - y$$

This means we can write:

$$x^k - y^k = m(x - y)$$

for some integer m.

Inductive Step:
We must prove the statement for $n = k + 1$:

$$x^{k+1} - y^{k+1} \text{ is divisible by } x - y$$

Start with $x^{k+1} - y^{k+1}$ and manipulate to introduce $x^k - y^k$:

$$\begin{aligned} x^{k+1} - y^{k+1} &= x^{k+1} - xy^k + xy^k - y^{k+1} \\ &= x(x^k - y^k) + y^k(x - y) \end{aligned}$$

Substitute the inductive hypothesis $x^k - y^k = m(x - y)$:

$$\begin{aligned} x^{k+1} - y^{k+1} &= x \cdot m(x - y) + y^k(x - y) \\ &= (x - y)(xm + y^k) \end{aligned}$$

Since x, y, m, k are all integers, $M = xm + y^k$ is an integer.
Therefore:

$$x^{k+1} - y^{k+1} = M(x - y)$$

This shows $x^{k+1} - y^{k+1}$ is divisible by $x - y$. ✓

Conclusion:
By mathematical induction, $x^n - y^n$ is divisible by $x - y$ for all positive integers n.

□

Note: This problem demonstrates the crossover between Induction and Proofs topics in HSC Extension 2.

Takeaways 2.14

- **Strategic Addition/Subtraction:** Add and subtract xy^k to create terms involving $x^k - y^k$ and $x - y$
- **Factorization:** Extract common factor $(x - y)$ after rearrangement
- **Induction Crossover:** Problem appears in both HSC-Induction and HSC-Proofs collections, showing technique overlap
- **Alternative Formula:** Result leads to $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$

Problem 2.15: Hard

For $n \in \mathbb{Z}$, prove that:

(a) n is divisible by 6 if and only if n is divisible by 2 and 3.

(b) $n^3 - n$ is divisible by 6.

Solution 2.15

Part (a): Biconditional Proof
Forward ($\implies$): If $6 \mid n$, then $2 \mid n$ and $3 \mid n$.

Proof. Assume $6 \mid n$. Then $n = 6k$ for some integer k.
Write $n = 6k = 2(3k)$. Since $3k$ is an integer, $2 \mid n$.
Write $n = 6k = 3(2k)$. Since $2k$ is an integer, $3 \mid n$. □ □

Reverse ($\impliedby$): If $2 \mid n$ and $3 \mid n$, then $6 \mid n$.

Proof. Assume $2 \mid n$ and $3 \mid n$.
Then $n = 2a$ and $n = 3b$ for some integers a, b.
From $n = 2a$, n is even. From $n = 3b$, we have $2a = 3b$.
Since LHS is even, RHS $3b$ must be even. Since 3 is odd, b must be even.
Write $b = 2c$ for some integer c.
Then:

$$n = 3b = 3(2c) = 6c$$

Since c is an integer, $6 \mid n$. □ □

Part (b): Using Part (a)
Goal: Prove $6 \mid (n^3 - n)$.
By part (a), sufficient to show $2 \mid (n^3 - n)$ and $3 \mid (n^3 - n)$.
Step 1: Factor

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

This is the product of three consecutive integers.
Step 2: Prove $2 \mid (n^3 - n)$
Among any three consecutive integers, at least one is even.
Therefore, $(n-1)n(n+1)$ contains an even factor, so $2 \mid (n^3 - n)$. ✓
Step 3: Prove $3 \mid (n^3 - n)$
Among any three consecutive integers, exactly one is divisible by 3.
Therefore, $(n-1)n(n+1)$ contains a factor divisible by 3, so $3 \mid (n^3 - n)$. ✓
Conclusion
Since $2 \mid (n^3 - n)$ and $3 \mid (n^3 - n)$, and $\gcd(2, 3) = 1$, by part (a):

$$6 \mid (n^3 - n)$$

□

Takeaways 2.15

- **Coprime Divisibility:** If $\gcd(a, b) = 1$ and both $a \mid n$ and $b \mid n$, then $ab \mid n$
- **Consecutive Integer Properties:** Among k consecutive integers, exactly one is divisible by k
- **Multi-part Strategy:** Part (b) leverages part (a) to simplify proof (check divisibility by 2 and 3 separately)
- **Factorization:** $n^3 - n = (n-1)n(n+1)$ reveals structure as consecutive integer product

3 Part 2: Problems with Hints and Sketches

The following problems provide strategic hints and solution sketches. Attempt each problem independently before consulting the hint. The sketches outline key steps but leave details for you to complete—use them to check your approach and fill in any gaps in your reasoning.

Easy Problems (5 problems)

Problem 3.1: Easy

Prove that the expression $a^3 - a + 1$ is odd for all positive integer values of a.

Hint: Consider factoring $a^3 - a$ as a product of consecutive integers. What can you say about the parity of any product of consecutive integers?
Alternatively, try proof by cases: analyze when a is even and when a is odd separately.

Solution Sketch 3.1

Method 1 (Factorization - Elegant):
Factor the expression:

$$\begin{aligned} a^3 - a + 1 &= a(a^2 - 1) + 1 \\ &= a(a-1)(a+1) + 1 \\ &= (a-1)a(a+1) + 1 \end{aligned}$$

The product $(a-1)a(a+1)$ is the product of three consecutive integers. In any set of consecutive integers, at least one must be even, so the product is even. Let $(a-1)a(a+1) = 2k$ for some integer k.
Therefore, $a^3 - a + 1 = 2k + 1$, which is odd by definition.

Method 2 (Cases):
Case 1: If $a = 2m$ (even), then $a^3 - a + 1 = 8m^3 - 2m + 1 = 2(4m^3 - m) + 1$ (odd).
Case 2: If $a = 2m + 1$ (odd), then expanding shows $a^3 - a + 1 = 2(\text{integer}) + 1$ (odd).
In both cases, the expression is odd. $\square$

Problem 3.2: Easy

If a is rational and b is irrational, prove that $a + b$ is irrational.

Hint: Use proof by contradiction. Assume $a + b$ is rational, then solve for b in terms of rational numbers. What property of rational numbers does this contradict?

Solution Sketch 3.2

Proof by Contradiction:
Assume, for contradiction, that $a + b$ is rational.
Since a is rational and $a + b$ is rational (by assumption), we can write:

$$a = \frac{p}{q} \quad \text{where } p, q \in \mathbb{Z}, q \neq 0$$
$$a + b = \frac{r}{s} \quad \text{where } r, s \in \mathbb{Z}, s \neq 0$$

Solving for b:

$$b = (a + b) - a = \frac{r}{s} - \frac{p}{q} = \frac{rq - ps}{sq}$$

Since r, q, p, s are all integers and $sq \neq 0$, this shows b is expressible as a ratio of two integers.
Therefore, b must be rational, which **contradicts** the given condition that b is irrational.
Hence, our assumption was false, and $a + b$ must be irrational. $\square$

Problem 3.3: Easy

Prove that an irrational number raised to the power of an irrational number can be rational, by considering $\sqrt{2}^{\sqrt{2}}$. You may assume $\sqrt{2}$ is irrational.

Hint: Consider $\alpha = \sqrt{2}^{\sqrt{2}}$. By the Law of Excluded Middle, α is either rational or irrational. Examine both cases:

- If α is rational, you're done immediately.
- If α is irrational, compute $\alpha^{\sqrt{2}}$ and simplify.

This is a **non-constructive** existence proof—you prove something exists without determining which case actually holds!

Solution Sketch 3.3

Proof by Cases:

Let $\alpha = \sqrt{2}^{\sqrt{2}}$. We consider two exhaustive cases:

Case 1: If $\alpha = \sqrt{2}^{\sqrt{2}}$ is rational, then we have found irrational base $\sqrt{2}$ and irrational exponent $\sqrt{2}$ such that $\sqrt{2}^{\sqrt{2}}$ is rational. Done.

Case 2: If $\alpha = \sqrt{2}^{\sqrt{2}}$ is irrational, consider:

$$\begin{aligned}
\alpha^{\sqrt{2}} &= \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} \\
&= \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} \quad \text{(exponent law)} \\
&= \sqrt{2}^{2} \\
&= 2
\end{aligned}$$

Since 2 is rational and both α (irrational by case assumption) and $\sqrt{2}$ (given as irrational) are irrational, we have found an example.

Conclusion: In either case, there exist irrational numbers a and b such that a^b is rational. □

Note: This proof doesn't tell us whether $\sqrt{2}^{\sqrt{2}}$ is actually rational or irrational—and we don't need to know! This is the beauty of non-constructive existence proofs.

Problem 3.4: Easy

Prove that for positive integers a, b with $a > 1$, either b is not divisible by a or $b + 1$ is not divisible by a (or both).

Hint: Use proof by contradiction. Assume both $a|b$ and $a|(b + 1)$. What does this tell you about $a|[(b + 1) - b]$? What can you conclude about a?

Solution Sketch 3.4

Proof by Contradiction:
The statement is equivalent to: "It is not the case that both $a|b$ and $a|(b + 1)$."
Assume, for contradiction, that **both** $a|b$ and $a|(b + 1)$.
Then there exist integers k_1 and k_2 such that:

$$b = ak_1$$
$$b + 1 = ak_2$$

Subtracting the first equation from the second:

$$(b + 1) - b = ak_2 - ak_1$$

$$1 = a(k_2 - k_1)$$

Let $K = k_2 - k_1 \in \mathbb{Z}$. Then $1 = aK$, which means a divides 1.
Since a is a positive integer, the only positive divisor of 1 is 1 itself. Therefore, $a = 1$.
This **contradicts** the given condition that $a > 1$.
Hence, our assumption must be false, and at least one of b or $b + 1$ is not divisible by a.
□

Problem 3.5: Easy

Prove that for all integers $n \geq 3$, if $2^n - 1$ is prime, then n cannot be even.

Hint: Use proof by contrapositive. Instead of proving "$P \implies Q$", prove "$\neg Q \implies \neg P$". That is, prove: "If n is even (and $n \geq 3$), then $2^n - 1$ is composite." Write $n = 2k$ and factor $2^{2k} - 1$ as a difference of squares.

Solution Sketch 3.5

Proof by Contrapositive:
We prove the contrapositive: If n is even (with $n \geq 3$), then $2^n - 1$ is composite.
Assume n is even. Then $n = 2k$ for some integer k.
Since $n \geq 3$ and n is even, we have $n \geq 4$, so $k \geq 2$.
Substitute:

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

Factor as difference of squares:

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

Since $k \geq 2$:

- $2^k \geq 4$, so $2^k - 1 \geq 3 > 1$
- $2^k \geq 4$, so $2^k + 1 \geq 5 > 1$

Both factors are integers strictly greater than 1, so their product is composite.
Therefore, $2^n - 1$ is composite.

By contrapositive, if $2^n - 1$ is prime, then n cannot be even. $\square$

Note: This is why Mersenne primes have the form $2^p - 1$ where p itself is prime (though not all such numbers are prime).

Medium Problems (5 problems)

Problem 3.6: Medium

Prove that $(2^m - 1)^2 - 1$ is divisible by 2^{m+1} for all integers $m \geq 1$.

Hint: Expand the perfect square $(2^m - 1)^2$ algebraically, then simplify. Try to factor out 2^{m+1} from the resulting expression.

Solution Sketch 3.6

Let $E = (2^m - 1)^2 - 1$.
Step 1: Expand the square:

$$\begin{aligned} E &= (2^m)^2 - 2(2^m) + 1 - 1 \\ &= 2^{2m} - 2^{m+1} + 1 - 1 \\ &= 2^{2m} - 2^{m+1} \end{aligned}$$

Step 2: Factor out 2^{m+1}:
Note that $2^{2m} = 2^{m+1} \cdot 2^{m-1}$ (using exponent laws).
Therefore:

$$\begin{aligned} E &= 2^{m+1} \cdot 2^{m-1} - 2^{m+1} \cdot 1 \\ &= 2^{m+1}(2^{m-1} - 1) \end{aligned}$$

Step 3: Conclude divisibility:
Since $m \geq 1$, we have $m - 1 \geq 0$, so 2^{m-1} is an integer. Thus $(2^{m-1} - 1)$ is an integer.
Therefore, $E = 2^{m+1} \cdot k$ where $k = 2^{m-1} - 1 \in \mathbb{Z}$.
By definition, $(2^m - 1)^2 - 1$ is divisible by 2^{m+1}. $\square$

Problem 3.7: Medium

Prove that there are no positive integers x, y such that $x^2 - y^2 = 1$.

Hint: Factor the left side as a difference of squares: $(x-y)(x+y) = 1$.
For this product to equal 1, what must be true about the integer factors $(x-y)$ and $(x+y)$?
Consider all possible integer factor pairs of 1.

Solution Sketch 3.7

Factor the equation:

$$x^2 - y^2 = 1 \implies (x-y)(x+y) = 1$$

Since x and y are integers, both $(x-y)$ and $(x+y)$ are integers.
For the product of two integers to equal 1, the only possibilities are:

- $x - y = 1$ and $x + y = 1$, or
- $x - y = -1$ and $x + y = -1$

Case 1: $x - y = 1$ and $x + y = 1$
Adding these equations: $2x = 2$, so $x = 1$.
Substituting back: $1 + y = 1$, so $y = 0$.
Since $y = 0$ is not a positive integer, this case fails.

Case 2: $x - y = -1$ and $x + y = -1$
Adding these equations: $2x = -2$, so $x = -1$.
Since $x = -1$ is not a positive integer, this case fails.

Conclusion: Neither case yields a solution with both x and y positive integers.
Therefore, there are no positive integers x, y such that $x^2 - y^2 = 1$. $\square$

Problem 3.8: Medium

Prove that a three-digit number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Hint: Let $N = 100a + 10b + c$ where a, b, c are the digits.
Rewrite this as $N = 9(11a + b) + (a + b + c)$ to establish the relationship between N and the digit sum.
Then prove both directions of the biconditional using this relationship.

Solution Sketch 3.8

Let $N = 100a + 10b + c$ be a three-digit number with digits a, b, c.
Let $S = a + b + c$ be the sum of digits.

Key Relationship:
Rewrite N:

$$\begin{aligned} N &= 100a + 10b + c \\ &= (99a + a) + (9b + b) + c \\ &= 9(11a + b) + (a + b + c) \\ &= 9(11a + b) + S \end{aligned}$$

Therefore: $N - S = 9(11a + b)$, which means $N \equiv S \pmod 9$.

Direction 1 ($\Rightarrow$): If $9|N$, then $9|S$.
If $N \equiv 0 \pmod 9$, then from $N \equiv S \pmod 9$, we get $S \equiv 0 \pmod 9$.
Thus $9|S$.

Direction 2 ($\Leftarrow$): If $9|S$, then $9|N$.
If $S \equiv 0 \pmod 9$, then from $N \equiv S \pmod 9$, we get $N \equiv 0 \pmod 9$.
Thus $9|N$.

Both directions proven, so the biconditional holds. $\square$

Note: This proof generalizes to all positive integers and divisibility by 9. The key is the modular relationship $N \equiv S \pmod 9$.

Problem 3.9: Medium

Consider the region $\mathcal{R}$ in the complex plane defined by $|z - (2\sqrt{3} + 2i)| \leq 2$.

(a) Describe the region $\mathcal{R}$ geometrically (what shape? center? radius?).

(b) Find the maximum and minimum values of $\arg(z)$ for $z \in \mathcal{R}$, where $-\pi < \arg(z) \leq \pi$.

(c) Find the complex number z associated with the maximum argument in part (b) in the form $x + iy$.

Hint: (a) The inequality $|z - w| \leq r$ represents a disk (filled circle) in the complex plane. (b) Find $\arg(C)$ where $C = 2\sqrt{3} + 2i$ is the center. The max/min arguments occur at tangent lines from the origin to the circle. Use the right triangle formed by the origin, center, and tangent point. (c) The point with maximum argument lies on the ray from O with angle $\arg_{\max}$ found in (b), at distance $\sqrt{|OC|^2 - r^2}$ from origin.

Solution Sketch 3.9

(a) Geometric Description:
The region is a closed disk (circle plus interior) with:

- Center: $C = 2\sqrt{3} + 2i$ (which is $(2\sqrt{3}, 2)$ in Cartesian coordinates)
- Radius: $r = 2$

Distance from origin to center: $|OC| = \sqrt{(2\sqrt{3})^2 + 2^2} = \sqrt{12+4} = 4$.
Since $|OC| = 4 > r = 2$, the origin lies outside the circle.

(b) Max and Min Arguments:
The argument of the center is:

$$\arg(C) = \arctan\left(\frac{2}{2\sqrt{3}}\right) = \arctan\left(\frac{1}{\sqrt{3}}\right) = \frac{\pi}{6}$$

The tangent lines from O to the circle create a right triangle with:

- Hypotenuse: $|OC| = 4$
- Opposite side (radius): $r = 2$

The angle θ from OC to the tangent satisfies:

$$\sin\theta = \frac{r}{|OC|} = \frac{2}{4} = \frac{1}{2} \implies \theta = \frac{\pi}{6}$$

Therefore:

$$\arg_{\max} = \frac{\pi}{6} + \frac{\pi}{6} = \frac{\pi}{3}$$
$$\arg_{\min} = \frac{\pi}{6} - \frac{\pi}{6} = 0$$

(c) Complex Number for Max Argument:
The tangent point distance from origin:

$$|OP| = \sqrt{|OC|^2 - r^2} = \sqrt{16-4} = \sqrt{12} = 2\sqrt{3}$$

The point lies on the ray with argument $\pi/3$:

$$\begin{aligned} z &= 2\sqrt{3} \cdot e^{i\pi/3} = 2\sqrt{3}\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) \\ &= 2\sqrt{3}\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\ &= \sqrt{3} + 3i \end{aligned}$$

Answer: $z = \sqrt{3} + 3i$. $\square$

Problem 3.10: Medium

Prove that x is even if and only if x^2 is even (for integer x).

Hint: This is a biconditional (iff) statement requiring two proofs:

- Direction 1: If x is even, then x^2 is even (direct proof).
- Direction 2: If x^2 is even, then x is even (try contrapositive: if x is odd, then x^2 is odd).

Solution Sketch 3.10

Direction 1 ($\Rightarrow$): If x is even, then x^2 is even.
Assume x is even. Then $x = 2k$ for some integer k.
Therefore:

$$x^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

Since $2k^2$ is an integer, x^2 is even by definition.

Direction 2 ($\Leftarrow$): If x^2 is even, then x is even.
We prove the contrapositive: If x is odd, then x^2 is odd.
Assume x is odd. Then $x = 2k + 1$ for some integer k.
Therefore:

$$\begin{aligned} x^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Since $2k^2 + 2k$ is an integer, x^2 is odd by definition.
By contrapositive, if x^2 is even, then x must be even.

Conclusion: Both directions proven, so x is even $\iff$ x^2 is even. $\square$

Note: This result is fundamental in many irrationality proofs (e.g., $\sqrt{2}$ is irrational). If p is an odd prime and $p|x^2$, then $p|x$.

Hard Problems (5 problems)

Problem 3.11: Hard

Prove or disprove: If x and y are irrational numbers with $x \neq y$, then xy is irrational.

Hint: The statement is **false**. Find a counterexample using multiples of $\sqrt{2}$.
Consider $x = \sqrt{2}$ and $y = k\sqrt{2}$ for some rational $k \neq 1$. What is xy? Is it rational or irrational?

Solution Sketch 3.11

The statement is **false**. We disprove by counterexample.

Counterexample:
Let $x = \sqrt{2}$ and $y = 2\sqrt{2}$.

- **Check x is irrational:** $\sqrt{2}$ is irrational (well-known).
- **Check y is irrational:** $2\sqrt{2}$ is the product of rational 2 and irrational $\sqrt{2}$, so it's irrational.
- **Check $x \neq y$:** Clearly $\sqrt{2} \neq 2\sqrt{2}$ since $1 \neq 2$.
- **Compute xy:**
$$xy = (\sqrt{2})(2\sqrt{2}) = 2 \cdot (\sqrt{2})^2 = 2 \cdot 2 = 4$$
- **Check rationality of xy:** $4 = \frac{4}{1}$ is **rational**.

Since we found irrational numbers x and y with $x \neq y$ such that xy is rational, the original statement is **disproven**. $\square$

Note: This shows that the irrationals are not closed under multiplication. The rationals are closed under multiplication, but the irrationals are not.

Problem 3.12: Hard

Prove that there is no Pythagorean triple (a, b, c) where a and b (the two smallest numbers) are both even and c (the largest number) is odd.

Hint: Use proof by contradiction. Assume such a triple exists with $a = 2k$ and $b = 2m$ (both even) and c odd.
Substitute into the Pythagorean equation $a^2 + b^2 = c^2$ and analyze the parity of c^2. What can you conclude about the parity of c?

Solution Sketch 3.12

Proof by Contradiction:
Assume there exists a Pythagorean triple (a, b, c) where:

- $a^2 + b^2 = c^2$
- a and b are both even
- c is odd

Since a and b are even, write $a = 2k$ and $b = 2m$ for integers k, m.

Substitute into Pythagorean equation:

$$\begin{aligned}(2k)^2 + (2m)^2 &= c^2\\ 4k^2 + 4m^2 &= c^2\\ 4(k^2 + m^2) &= c^2\end{aligned}$$

Analyze parity of c^2:
The equation shows $c^2 = 4(k^2 + m^2)$, which is a multiple of 4.
In particular, c^2 is divisible by 2, so c^2 is **even**.

Derive parity of c:
If c were odd, then $c = 2n + 1$ for some integer n, and:

$$c^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$$

This shows c^2 would be **odd**, contradicting that c^2 is even.
Therefore, c must be **even**.

Contradiction:
We derived that c must be even, which contradicts our assumption that c is odd.
Hence, no such Pythagorean triple exists. $\square$

Problem 3.13: Hard

Prove or disprove: There exists a real number n such that $3^n + 4^n < 5^n$.

Hint: The statement is **true**. Try a few values: $n = 2$ gives $9 + 16 = 25 = 5^2$ (equality, not $<$).
Try $n = 3$: Is $3^3 + 4^3 < 5^3$? Calculate $27 + 64$ vs 125.
Alternatively, divide by 5^n to get $(3/5)^n + (4/5)^n < 1$ and analyze the function behavior.

Solution Sketch 3.13

The statement is **true**.

Proof by Example:
Try $n = 3$:

$$3^3 + 4^3 = 27 + 64 = 91$$
$$5^3 = 125$$

Since $91 < 125$, the inequality $3^3 + 4^3 < 5^3$ holds.
Therefore, $n = 3$ is a real number satisfying the inequality. $\square$

Alternative Proof (Analysis):
Divide the inequality by 5^n:

$$\left(\frac{3}{5}\right)^n + \left(\frac{4}{5}\right)^n < 1$$

Let $f(n) = \left(\frac{3}{5}\right)^n + \left(\frac{4}{5}\right)^n$.

- At $n = 2$: $f(2) = \frac{9}{25} + \frac{16}{25} = 1$ (equality)
- The derivative: $f'(n) = \left(\frac{3}{5}\right)^n \ln\left(\frac{3}{5}\right) + \left(\frac{4}{5}\right)^n \ln\left(\frac{4}{5}\right)$
  Since $\frac{3}{5} < 1$ and $\frac{4}{5} < 1$, both logarithms are negative, so $f'(n) < 0$.
- Therefore, $f(n)$ is strictly decreasing.

Since $f(2) = 1$ and f is strictly decreasing, for any $n > 2$, we have $f(n) < 1$.
Thus, the inequality holds for all $n > 2$. In particular, it holds for $n = 3$ (and infinitely many other values). $\square$

Note: This shows the power of the "divide by largest term" technique in inequality problems. The critical point is $n = 2$ where equality holds (Pythagorean triple: $3^2 + 4^2 = 5^2$).

Problem 3.14: Hard

Prove by induction that for all integers $n \geq 2$:

$$1^3 + 2^3 + \cdots + (n-1)^3 < \frac{n^4}{4} < 1^3 + 2^3 + \cdots + n^3$$

Hint: This is a "sandwich" inequality with two parts:

- LHS inequality: $\sum_{k=1}^{n-1} k^3 < \frac{n^4}{4}$ (needs induction)
- RHS inequality: $\frac{n^4}{4} < \sum_{k=1}^{n} k^3$ (can be proven directly)

Recall: $\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2 = \frac{n^2(n+1)^2}{4}$

For the LHS induction step, you'll need to show $\frac{k^4}{4} + k^3 < \frac{(k+1)^4}{4}$, which simplifies to $0 < 6k^2 + 4k + 1$.

Solution Sketch 3.14

Part 1: RHS Inequality (Direct Proof)
Show $\frac{n^4}{4} < \sum_{k=1}^{n} k^3$ for $n \geq 2$.
Using the sum formula:

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} = \frac{n^4 + 2n^3 + n^2}{4}$$

We need: $\frac{n^4}{4} < \frac{n^4+2n^3+n^2}{4}$
This simplifies to: $0 < 2n^3 + n^2 = n^2(2n+1)$
Since $n \geq 2 > 0$, this is clearly true. RHS proven. ✓

Part 2: LHS Inequality (Induction)
Prove $\sum_{k=1}^{n-1} k^3 < \frac{n^4}{4}$ for $n \geq 2$.

Base case ($n = 2$):

$$\sum_{k=1}^{1} k^3 = 1^3 = 1 < \frac{2^4}{4} = 4 \quad \checkmark$$

Inductive hypothesis: Assume $\sum_{k=1}^{m-1} k^3 < \frac{m^4}{4}$ for some $m \geq 2$.

Inductive step: Prove $\sum_{k=1}^{m} k^3 < \frac{(m+1)^4}{4}$.

$$\begin{aligned}\sum_{k=1}^{m} k^3 &= \sum_{k=1}^{m-1} k^3 + m^3 \\ &< \frac{m^4}{4} + m^3 \quad \text{(by IH)} \\ &= \frac{m^4 + 4m^3}{4}\end{aligned}$$

Need to show: $\frac{m^4+4m^3}{4} < \frac{(m+1)^4}{4}$
Equivalently: $m^4 + 4m^3 < (m+1)^4$
Expand RHS:

$$(m+1)^4 = m^4 + 4m^3 + 6m^2 + 4m + 1$$

So we need: $m^4 + 4m^3 < m^4 + 4m^3 + 6m^2 + 4m + 1$
Simplifies to: $0 < 6m^2 + 4m + 1$
This is true for all $m \geq 2$. ✓

By induction, LHS proven. Combining both parts, the full sandwich inequality holds. □

Problem 3.15: Hard

Prove by induction that $4^{n+1} + 6^n$ is divisible by 10 when n is an even positive integer.

Hint: Since n is even, let $n = 2k$ for $k \geq 1$. Prove by induction on k that $4^{2k+1} + 6^{2k}$ is divisible by 10.

For the inductive step:

- Express $4^{2(k+1)+1} + 6^{2(k+1)}$ as $16 \cdot 4^{2k+1} + 36 \cdot 6^{2k}$
- From IH: $6^{2k} = 10M - 4^{2k+1}$ for some integer M
- Substitute and factor out 10

Solution Sketch 3.15

Since n is an even positive integer, let $n = 2k$ where $k \in \mathbb{Z}^+$.
We prove by induction on k that $P(k)$: "$4^{2k+1} + 6^{2k}$ is divisible by 10" holds for all $k \geq 1$.

Base case ($k = 1$, i.e., $n = 2$):

$$4^{2(1)+1} + 6^{2(1)} = 4^3 + 6^2 = 64 + 36 = 100 = 10 \times 10$$

Divisible by 10. ✓

Inductive hypothesis:
Assume $P(k)$ holds: $4^{2k+1} + 6^{2k} = 10M$ for some integer M.
From this: $6^{2k} = 10M - 4^{2k+1}$

Inductive step:
Prove $P(k+1)$: $4^{2(k+1)+1} + 6^{2(k+1)}$ is divisible by 10.

$$\begin{aligned} 4^{2(k+1)+1} + 6^{2(k+1)} &= 4^{2k+3} + 6^{2k+2} \\ &= 4^2 \cdot 4^{2k+1} + 6^2 \cdot 6^{2k} \\ &= 16 \cdot 4^{2k+1} + 36 \cdot 6^{2k} \end{aligned}$$

Substitute $6^{2k} = 10M - 4^{2k+1}$ from IH:

$$\begin{aligned} &= 16 \cdot 4^{2k+1} + 36(10M - 4^{2k+1}) \\ &= 16 \cdot 4^{2k+1} + 360M - 36 \cdot 4^{2k+1} \\ &= 360M + (16 - 36) \cdot 4^{2k+1} \\ &= 360M - 20 \cdot 4^{2k+1} \\ &= 10(36M - 2 \cdot 4^{2k+1}) \end{aligned}$$

Since M and 4^{2k+1} are integers, $36M - 2 \cdot 4^{2k+1}$ is an integer.
Therefore, $4^{2(k+1)+1} + 6^{2(k+1)}$ is divisible by 10. ✓

By the principle of mathematical induction, $P(k)$ holds for all $k \geq 1$.
Therefore, $4^{n+1} + 6^n$ is divisible by 10 for all even positive integers n. □

Problem 3.16: Hard

Consider the sequence defined by $x_0 \in (0,1)$ and the recurrence

$$x_{n+1} = 4x_n(1 - x_n), \quad n \geq 0.$$

Known as the logistic map, this deceptively simple rule from dynamical systems models feedback in real contexts (population growth, supply–demand, etc.) and is a classic gateway to chaos. Even tiny changes in x_0 can produce dramatically different long-term behavior, making it a fascinating playground for exploration.

This problem guides you through key properties of this sequence using trigonometric substitutions, product identities, and periodicity analysis.

(i) Let $x_0 = \sin^2\theta$ for some $\theta \in \left(0, \frac{\pi}{2}\right)$. Prove by induction that for all $n \geq 0$,

$$x_n = \sin^2\left(2^n\theta\right).$$

(ii) Using the result from (i), show that for $n \geq 1$,

$$x_n = 4^n x_0 \prod_{k=0}^{n-1}(1 - x_k).$$

(iii) Take $x_0 = \sin^2\left(\frac{\pi}{7}\right)$. Show the sequence is periodic with period 3. Hence evaluate

$$P = \cos\left(\tfrac{\pi}{7}\right)\cos\left(\tfrac{2\pi}{7}\right)\cos\left(\tfrac{4\pi}{7}\right).$$

(iv) A sequence is periodic if it eventually repeats values. Show that the sequence x_n is periodic (or eventually periodic) if the starting angle θ_0 is a rational multiple of π. That means, if $x_0 = \sin^2(\theta_0)$, then a sufficient condition is $\theta_0 = \frac{p}{q}\pi$ with $p, q \in \mathbb{Z}$ for x_n to be eventually periodic.
Note that proving the reverse direction (the "only if" part) is more challenging.
(v) Discuss the behaviour when $x_0 = \frac{1}{2}$ Determine whether the sequence is periodic, eventually periodic, or convergent.

Hint: For (i), aim to express x_{k+1} in terms of x_k in a squared-trigonometric form and use induction. For (ii), turn the recurrence into a ratio to build a telescoping product. For (iii), use the angle-doubling description in (i) to show $x_3 = x_0$ when $\theta_0 = \frac{\pi}{7}$, and recall the classical identity involving $\cos\frac{\pi}{7}, \cos\frac{2\pi}{7}, \cos\frac{4\pi}{7}$. For (v), compute a few terms explicitly and look for eventual repetition or a fixed point.

Solution Sketch 3.16

(i) Base: $x_0 = \sin^2\theta$. Inductive step: if $x_k = \sin^2(2^k\theta)$, then

$$x_{k+1} = 4x_k(1-x_k) = 4\sin^2(2^k\theta)\cos^2(2^k\theta) = \sin^2(2^{k+1}\theta).$$

(ii) From $x_{k+1} = 4x_k(1-x_k)$, rearrange $(1-x_k) = \dfrac{x_{k+1}}{4x_k}$ and telescope:

$$\prod_{k=0}^{n-1}(1-x_k) = \frac{1}{4^n}\,\frac{x_n}{x_0} \;\Rightarrow\; x_n = 4^n x_0 \prod_{k=0}^{n-1}(1-x_k).$$

(iii) With $\theta_0 = \frac{\pi}{7}$, we have $x_3 = \sin^2\left(2^3\tfrac{\pi}{7}\right) = \sin^2\left(\tfrac{8\pi}{7}\right) = \sin^2\left(\tfrac{\pi}{7}\right) = x_0$, so the period is 3. The classical identity yields

$$\cos\left(\tfrac{\pi}{7}\right)\cos\left(\tfrac{2\pi}{7}\right)\cos\left(\tfrac{4\pi}{7}\right) = -\tfrac{1}{8}.$$

(iv) If $\theta_0 = \frac{p}{q}\pi$, the map $\theta \mapsto 2\theta$ cycles modulo π, so $x_q = x_0$; proving the converse (only-if) direction is subtler.
(v) With $x_0 = \frac{1}{2}$, $x_1 = 1$, $x_2 = 0$, and thereafter $x_n = 0$ for $n \geq 2$; hence the sequence is eventually periodic (fixed point 0).

Takeaways 3.1

- Trig substitution $x_n = \sin^2(2^n\theta)$ linearizes the logistic map. - The product identity follows from a telescoping ratio across iterates. - Rational multiples of π lead to periodic (or eventually periodic) behaviour; proving the converse is harder. - Classical identities like $\cos\frac{\pi}{7}\cos\frac{2\pi}{7}\cos\frac{4\pi}{7} = -\frac{1}{8}$ connect dynamics with trigonometric products.

Contact Information:

LinkedIn: https://www.linkedin.com/in/nguyenvuhung/

GitHub: https://github.com/vuhung16au/

Repository: https://github.com/vuhung16au/math-olympiad-ml/tree/main/HSC-Proofs