

MH1300 Foundations of Mathematics – Solutions

Final Examination, Academic Year 2019/2020, Semester 1

Compiled and typeset by QRS from the original handwritten solution

November 8, 2025

Summary

This paper examines core topics in discrete mathematics and introductory proof-writing, including properties of rational and irrational numbers, composite integers, formal logic, sets, parity and divisibility. Subsequent questions test fluency with mathematical induction, modular arithmetic, divisibility tests, and number-theoretic arguments using parity and congruences. The exam also covers symmetric difference and power sets, injectivity and surjectivity of functions on \mathbb{Z} , equality conditions in the triangle inequality, roots of unity in the complex plane, and basic properties of binary relations such as reflexivity, symmetry and transitivity. Several questions involve equivalence relations and classification of equivalence classes by parity, as well as the Euclidean algorithm for computing greatest common divisors. Most proofs can be handled using direct argument, proof by contradiction, induction and simple case analysis, while some parts require careful symbolic manipulation of logical statements or set expressions. Overall, the difficulty ranges from routine conceptual checks and counterexamples to moderately challenging proofs that combine multiple ideas (e.g. parity plus divisibility, or algebraic identities plus modular reasoning), and the indicative mark schemes highlight the key steps required for full credit.

Question 1**[18 marks]**

- (a) Suppose x, y, z are real numbers, x is irrational, and y is rational. Show that not both $xy + z$ and $xy - z$ are rational. [6 marks]
- (b) Let n be a positive integer, and n composite. Show that there exists a divisor m of n such that $1 < m < n$. [6 marks]
- (c) Consider the following logical argument. Use logical notation to write out each step and identify which rule of inference was used. [6 marks]

Solution.

- (a) **Proof by contradiction.**

Suppose the statement is false, i.e. assume that both $xy + z$ and $xy - z$ are rational.

By Theorem 4.2.2 of the lecture notes, the sum of any two rational numbers is rational.

Since both $xy + z$ and $xy - z$ are rational, their sum is rational:

$$(xy + z) + (xy - z) = 2xy \text{ is rational.}$$

By Ex. 4.2.16 in Tutorial 5, since $2xy$ is rational and $2y$ is rational (as y is rational), we have that

$$x = \frac{2xy}{2y}$$

is rational.

This contradicts the hypothesis that x is irrational.

Therefore, not both $xy + z$ and $xy - z$ can be rational. \square

- (b) **Proof by contradiction.**

Suppose, for contradiction, that there is no divisor m of n such that $1 < m < n$.

Since n is composite, we have $n = pq$ for some integers p, q with $1 < p < n$ and $1 < q < n$.

But this means p and q are divisors of n with $1 < p < n$ and $1 < q < n$, contradicting our assumption.

Therefore, there exists a divisor m of n such that $1 < m < n$. \square

- (c) **Logical argument structure.**

- | | | |
|----|--------------------------------|-------------------------|
| 1. | $S \vee P$ | (Premise) |
| 2. | $\neg(S \vee P) \rightarrow T$ | (Premise) |
| 3. | $\neg T$ | (Premise) |
| 4. | $\neg\neg(S \vee P)$ | (Modus Tollens on 2, 3) |
| 5. | $S \vee P$ | (Double negation on 4) |
| 6. | $\neg(\neg Q \wedge \neg R)$ | (Premise) |
| 7. | $Q \vee R$ | (De Morgan's law on 6) |

Each line is obtained from the previous ones using the indicated rule of inference or equivalence. □

Mark Scheme:

- (a)(i) Assume both $xy + z$ and $xy - z$ rational, deduce $2xy$ rational and hence x rational via division by $2y$, and state the contradiction with “ x irrational”. [4]
- (b) Use the definition of composite number to exhibit factors p, q with $1 < p < n$ and $1 < q < n$, and conclude that at least one such factor is a divisor m with $1 < m < n$. [5]
- (c) Correct symbolic translation of the premises and conclusion, correct identification of Modus Tollens, double negation and De Morgan's law in the steps, with a coherent linear argument. [5]

Question 2**[10 marks]**

- (a) **True or False:** There exist sets A and B such that $A \neq B$, $A \in B$, and $A \subseteq B$. Justify your answer. [3 marks]
- (b) **True or False:** For every integer n , the four numbers n, n^2, n^3, n^4 are not all of the same parity. Justify your answer. [3 marks]
- (c) **True or False:** There do not exist odd integers a, b such that $4 \mid (3a^2 + 7b^2)$. Justify your answer. [4 marks]

Solution.

- (a)
- True.**

Proof: Take $A = \{x\}$ for any element x , and $B = \{x, A\} = \{x, \{x\}\}$.

Then:

- $A \neq B$ since $\{x\} \neq \{x, \{x\}\}$.
- $A \in B$ since $\{x\} \in \{x, \{x\}\}$.
- $A \subseteq B$ since every element of A (which is just x) is in B .

Thus, such sets exist. □

- (b)
- False.**

Counterexample: Take $n = 2$. Then $n = 2$, $n^2 = 4$, $n^3 = 8$, $n^4 = 16$ are all even.

The statement claims these are not all of the same parity, but they are all even. So the statement is **false**. □

- (c)
- True.**

Proof by contradiction: Assume that there exist odd integers a, b such that $4 \mid (3a^2 + 7b^2)$.

Let $a = 2k + 1$ and $b = 2\ell + 1$ for integers k and ℓ .

Then

$$\begin{aligned}
 3a^2 + 7b^2 &= 3(2k + 1)^2 + 7(2\ell + 1)^2 \\
 &= 3(4k^2 + 4k + 1) + 7(4\ell^2 + 4\ell + 1) \\
 &= 12k^2 + 12k + 3 + 28\ell^2 + 28\ell + 7 \\
 &= 4(3k^2 + 3k + 7\ell^2 + 7\ell) + 10 \\
 &= 4(3k^2 + 3k + 7\ell^2 + 7\ell + 2) + 2.
 \end{aligned}$$

So

$$3a^2 + 7b^2 \equiv 2 \pmod{4},$$

meaning $4 \nmid (3a^2 + 7b^2)$.

This contradicts the assumption. Therefore, there do not exist odd integers a, b such that $4 \mid (3a^2 + 7b^2)$, so the statement is true. □

Mark Scheme:

- (a) Correct choice of A, B with $A \neq B$, $A \in B$ and $A \subseteq B$, and brief justification of each property. [3]
- (b) Suitable integer n (e.g. $n = 2$) with explicit calculation of n, n^2, n^3, n^4 and observation that all have the same parity, contradicting the claim. [3]
- (c) Representation of odd integers a, b as $2k + 1, 2\ell + 1$, algebraic expansion to show $3a^2 + 7b^2 \equiv 2 \pmod{4}$, and clear contradiction with $4 \mid (3a^2 + 7b^2)$. [4]

Question 3**[15 marks]**

- (a) Prove by induction: $1 + 5 + 9 + \cdots + (4n - 3) = 2n^2 - n$ for all $n \geq 1$. [7 marks]
 (b) Prove by induction: $3^{4n+1} - 5^{2n-1}$ is divisible by 7 for all $n \geq 1$. [8 marks]

Solution.

- (a) Proof by mathematical induction.**

Let $P(n)$ denote the statement

$$1 + 5 + 9 + \cdots + (4n - 3) = 2n^2 - n.$$

Base case $P(1)$:

$$\text{LHS} = 1, \quad \text{RHS} = 2(1)^2 - 1 = 2 - 1 = 1.$$

So $P(1)$ holds.**Inductive step:** Assume $P(k)$ holds, i.e.

$$1 + 5 + 9 + \cdots + (4k - 3) = 2k^2 - k.$$

We need to show $P(k + 1)$ holds:

$$\begin{aligned} \text{LHS of } P(k + 1) &= 1 + 5 + 9 + \cdots + (4k - 3) + (4k + 1) \\ &= (2k^2 - k) + (4k + 1) \quad (\text{by inductive hypothesis}) \\ &= 2k^2 + 3k + 1. \end{aligned}$$

On the other hand,

$$\begin{aligned} \text{RHS of } P(k + 1) &= 2(k + 1)^2 - (k + 1) \\ &= 2(k^2 + 2k + 1) - k - 1 \\ &= 2k^2 + 4k + 2 - k - 1 \\ &= 2k^2 + 3k + 1. \end{aligned}$$

Thus $\text{LHS} = \text{RHS}$ for $P(k + 1)$.By mathematical induction, $P(n)$ holds for all $n \geq 1$. □

- (b) Proof by mathematical induction.**

Let $P(n)$ denote the statement “ $3^{4n+1} - 5^{2n-1}$ is divisible by 7” for $n \geq 1$.**Base case** $P(1)$:

$$3^5 - 5^1 = 243 - 5 = 238 = 7 \times 34.$$

So $3^5 - 5$ is divisible by 7, and $P(1)$ holds.**Inductive step:** Assume $P(k)$ holds, i.e. $7 \mid (3^{4k+1} - 5^{2k-1})$.Let $3^{4k+1} - 5^{2k-1} = 7\ell$ for some integer ℓ .

We need to show $P(k+1)$ holds:

$$\begin{aligned} 3^{4(k+1)+1} - 5^{2(k+1)-1} &= 3^{4k+5} - 5^{2k+1} \\ &= 3^{4k+1} \cdot 3^4 - 5^{2k-1} \cdot 5^2 \\ &= 81 \cdot 3^{4k+1} - 25 \cdot 5^{2k-1}. \end{aligned}$$

Rewrite as

$$\begin{aligned} 3^{4k+5} - 5^{2k+1} &= 77 \cdot 3^{4k+1} + 4 \cdot 3^{4k+1} - 25 \cdot 5^{2k-1} \\ &= 77 \cdot 3^{4k+1} + 4(3^{4k+1} - 5^{2k-1}) - 4 \cdot 5^{2k-1} + 25 \cdot 5^{2k-1} \\ &= 77 \cdot 3^{4k+1} + 4 \cdot 7\ell + 21 \cdot 5^{2k-1} \\ &= 7(11 \cdot 3^{4k+1} + 4\ell + 3 \cdot 5^{2k-1}). \end{aligned}$$

Thus $3^{4(k+1)+1} - 5^{2(k+1)-1}$ is divisible by 7, so $P(k+1)$ holds.

By mathematical induction, $P(n)$ holds for all $n \geq 1$. □

Mark Scheme:

- (a) Correct formulation of $P(n)$, verification of $P(1)$, substitution of the inductive hypothesis into the $(k+1)$ -case, and algebraic simplification to show LHS = RHS, followed by an induction conclusion. [7]
- (b) Correct base case $n = 1$, clear inductive hypothesis $P(k)$, algebraic manipulation of $3^{4(k+1)+1} - 5^{2(k+1)-1}$ to factor out $3^{4k+1} - 5^{2k-1}$, use of the hypothesis to factor out 7, and final statement that the expression is divisible by 7. [8]

Question 4**[15 marks]**

- (a) Prove that $(n-1)^3 + n^3 + (n+1)^3$ is divisible by 9 for any integer n . [5 marks]
- (b) Prove that an integer m is divisible by 4 if and only if the last two digits of m form a number divisible by 4. [5 marks]
- (c) Let p be a positive integer with the property that

$$\forall a, b \in \mathbb{Z}, (p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b)).$$

Prove that \sqrt{p} is irrational. [5 marks]

Solution.

(a) **Proof.**

Expanding:

$$\begin{aligned} (n-1)^3 + n^3 + (n+1)^3 &= (n^3 - 3n^2 + 3n - 1) + n^3 + (n^3 + 3n^2 + 3n + 1) \\ &= 3n^3 + 6n \\ &= 3n(n^2 + 2). \end{aligned}$$

By the Quotient–Remainder Theorem, $n \equiv 0, 1$, or $2 \pmod{3}$.

Case 1: $n = 3q$. Then $3n(n^2 + 2) = 9q(n^2 + 2)$ is divisible by 9.

Case 2: $n = 3q + 1$. Then

$$n^2 + 2 = (3q + 1)^2 + 2 = 9q^2 + 6q + 3 = 3(3q^2 + 2q + 1),$$

so

$$3n(n^2 + 2) = 9(3q + 1)(3q^2 + 2q + 1)$$

is divisible by 9.

Case 3: $n = 3q + 2$. Then

$$n^2 + 2 = (3q + 2)^2 + 2 = 9q^2 + 12q + 6 = 3(3q^2 + 4q + 2),$$

so

$$3n(n^2 + 2) = 9(3q + 2)(3q^2 + 4q + 2)$$

is divisible by 9.

In all cases, $(n-1)^3 + n^3 + (n+1)^3$ is divisible by 9. □

(b) **Proof.**

Let m have digits $d_k d_{k-1} \cdots d_1 d_0$ in base 10. Then

$$m = 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10d_1 + d_0.$$

Note that for $k \geq 2$, $10^k = 100 \cdot 10^{k-2}$ is divisible by 4.

Therefore,

$$m \equiv 10d_1 + d_0 \pmod{4}.$$

The last two digits form the number $10d_1 + d_0$. Thus, $4 \mid m$ if and only if $4 \mid (10d_1 + d_0)$, i.e. if and only if the last two digits form a number divisible by 4. \square

(c) **Proof by contradiction.**

Assume \sqrt{p} is rational. Then $\sqrt{p} = \frac{r}{s}$ for some integers r, s with $s \neq 0$ and $\gcd(r, s) = 1$.

Then $p = \frac{r^2}{s^2}$, so $r^2 = ps^2$.

Since $p \mid ps^2$, we have $p \mid r^2$.

By the property of p , from $p \mid r^2$ it follows that $p \mid r$.

Let $r = pt$ for some integer t . Then

$$s^2p = r^2 = (pt)^2 = p^2t^2,$$

so $s^2 = pt^2$.

Thus $p \mid s^2$, and again by the property of p , $p \mid s$.

But if $p \mid r$ and $p \mid s$, this contradicts $\gcd(r, s) = 1$.

Therefore, \sqrt{p} is irrational. \square

Mark Scheme:

- (a) Algebraic expansion of $(n-1)^3 + n^3 + (n+1)^3$, factorisation as $3n(n^2 + 2)$, and case analysis modulo 3 to show $n(n^2 + 2)$ is always a multiple of 3. [5]
- (b) Decomposition of m into base-10 digits, observation that all powers 10^k with $k \geq 2$ are multiples of 4, reduction $m \equiv 10d_1 + d_0 \pmod{4}$, and equivalence between divisibility of m and its last two digits by 4. [5]
- (c) Rational representation $\sqrt{p} = r/s$, derivation of $r^2 = ps^2$, use of the given property to show p divides both r and s , contradiction with $\gcd(r, s) = 1$, and conclusion that \sqrt{p} is irrational. [5]

Question 5**[12 marks]**

- (a) (i) Prove that $A \triangle B = (A \setminus B) \cup (B \setminus A)$. [5 marks]
(ii) Show that $A = B$ if and only if $A \triangle B = \emptyset$. [3 marks]
- (b) Suppose $|A| = k$ and $|D| = k$. Find $|P(A \times D)|$ and $|P(P(D))|$ in terms of k . [2 marks]
- (c) Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by $f(n) = 5n + 2$. Determine if f is injective and if f is surjective. Justify. [2 marks]

Solution.

- (a) (i)
- Proof.**

Recall that

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Let $x \in A \triangle B$. Then $x \in (A \setminus B)$ or $x \in (B \setminus A)$.By definition, $x \in (A \triangle B)$ if and only if $x \in (A \setminus B) \cup (B \setminus A)$.

Now note that

$$(A \setminus B) \cap (B \setminus A) = \emptyset,$$

so

$$(A \setminus B) \cup (B \setminus A) = ((A \setminus B) \setminus (B \setminus A)) \cup ((B \setminus A) \setminus (A \setminus B)) = (A \setminus B) \cup (B \setminus A) = A \triangle B.$$

Hence $A \triangle B = (A \setminus B) \cup (B \setminus A)$. □

- (ii)
- Proof.**

 (\Rightarrow) If $A = B$, then $A \setminus B = \emptyset$ and $B \setminus A = \emptyset$, so

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = \emptyset.$$

 (\Leftarrow) If $A \triangle B = \emptyset$, then

$$(A \setminus B) \cup (B \setminus A) = \emptyset.$$

Thus $A \setminus B = \emptyset$ and $B \setminus A = \emptyset$, which means $A \subseteq B$ and $B \subseteq A$. Hence $A = B$. □

- (b)
- Finding cardinalities.**

Since $|A| = k$ and $|D| = k$, we have $|A \times D| = k \cdot k = k^2$.

Therefore,

$$|P(A \times D)| = 2^{k^2}.$$

Similarly, $|D| = k$ implies $|P(D)| = 2^k$, and thus

$$|P(P(D))| = 2^{|P(D)|} = 2^{2^k}.$$

So

$$\boxed{|P(A \times D)| = 2^{k^2}, \quad |P(P(D))| = 2^{2^k}}.$$

- (c) **Injectivity and surjectivity of $f(n) = 5n + 2$.**

Injective: Suppose $f(n) = f(m)$. Then

$$5n + 2 = 5m + 2 \quad \Rightarrow \quad 5n = 5m \quad \Rightarrow \quad n = m.$$

Thus f is **injective**.

Surjective: Suppose $y \in \mathbb{Z}$. We would need some $n \in \mathbb{Z}$ with $5n + 2 = y$, i.e. $n = \frac{y-2}{5}$. For n to be an integer, we need $5 \mid (y-2)$. Not every integer y satisfies this (e.g. $y = 0$ gives $n = -\frac{2}{5}$, not an integer). Thus f is **not surjective**.

Therefore

f is injective but not surjective.

Mark Scheme:

- (a)(i) Use of the definition $A \triangle B = (A \setminus B) \cup (B \setminus A)$, observation that $(A \setminus B) \cap (B \setminus A) = \emptyset$, and correct simplification of $(A \setminus B) \triangle (B \setminus A)$ to $A \triangle B$. [5]
- (a)(ii) Argument that $A = B$ implies both $A \setminus B$ and $B \setminus A$ are empty, and conversely that $A \triangle B = \emptyset$ implies $A \subseteq B$ and $B \subseteq A$, hence $A = B$. [3]
- (b) Correct use of $|A \times D| = |A||D|$ and $|P(S)| = 2^{|S|}$ to obtain 2^{k^2} and 2^{2^k} . [2]
- (c) Verification of injectivity via $f(n) = f(m) \Rightarrow n = m$, and demonstration that not every $y \in \mathbb{Z}$ can be written as $5n + 2$, so f is not surjective. [2]

Question 6**[15 marks]**

- (a) If $z, w \in \mathbb{C}$, find the condition for $|z + w| = |z| + |w|$. [5 marks]
- (b) Find all cube roots of 1. [5 marks]
- (c) **True or False:** If R_1 and R_2 are transitive relations, then $R_1 \cup R_2$ is transitive. Justify your answer. [5 marks]

Solution.

- (a) Condition for equality.**

By the triangle inequality, $|z + w| \leq |z| + |w|$ always holds.

Equality $|z + w| = |z| + |w|$ holds if and only if z and w point in the same direction in the complex plane, i.e. when there exists $\lambda \geq 0$ such that

$$z = \lambda w$$

(or equivalently, $\frac{z}{w}$ is a nonnegative real number when $w \neq 0$). The equality also trivially holds if one of z, w is zero.

| |
|--|
| $ z + w = z + w \iff z \text{ and } w \text{ have the same argument or one is zero.}$ |
|--|

- (b) Cube roots of 1.**

Let $z^3 = 1 = e^{i \cdot 0}$.

Using De Moivre's formula, the cube roots of 1 are given by

$$z_k = e^{i \cdot 2\pi k/3}, \quad k = 0, 1, 2.$$

Explicitly,

$$\begin{aligned} z_0 &= e^{i \cdot 0} = 1, \\ z_1 &= e^{i \cdot 2\pi/3} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i \frac{\sqrt{3}}{2}, \\ z_2 &= e^{i \cdot 4\pi/3} = \cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i \frac{\sqrt{3}}{2}. \end{aligned}$$

| |
|--|
| $z_0 = 1, \quad z_1 = -\frac{1}{2} + i \frac{\sqrt{3}}{2}, \quad z_2 = -\frac{1}{2} - i \frac{\sqrt{3}}{2}.$ |
|--|

- (c) False.**

Counterexample: Let $R_1 = \{(0, 1)\}$ and $R_2 = \{(1, 2)\}$ on \mathbb{Z} . Each relation on its own is transitive (vacuously, since there are no pairs $(a, b), (b, c)$ both in R_1 or both in R_2 with b matching).

However,

$$R_1 \cup R_2 = \{(0, 1), (1, 2)\}$$

is not transitive, since $(0, 1) \in R_1 \cup R_2$ and $(1, 2) \in R_1 \cup R_2$, but $(0, 2) \notin R_1 \cup R_2$.

Hence $R_1 \cup R_2$ need not be transitive.

False.

□

Mark Scheme:

- (a) Statement of the triangle inequality, correct characterisation that equality holds iff z and w are nonnegative real multiples of each other (or one is zero), and a brief justification. [5]
- (b) Application of De Moivre's formula to obtain $e^{2\pi ik/3}$, $k = 0, 1, 2$, and writing them explicitly in standard $a + bi$ form. [5]
- (c) Construction of transitive R_1, R_2 whose union contains (a, b) and (b, c) but not (a, c) , and clear explanation why this shows $R_1 \cup R_2$ is not transitive. [5]

Question 7**[15 marks]**

- (a) Define a relation R on \mathbb{N} by $(a, b) \in R$ iff $a^2 + b^2$ is even.
- (i) Show that R is an equivalence relation. [6 marks]
- (ii) Find all equivalence classes. [4 marks]
- (b) Use the Euclidean algorithm to find $\gcd(224, 126)$. [5 marks]

Solution.

- (a) (i) **Showing R is an equivalence relation.**

Reflexive: Let $a \in \mathbb{N}$. Then

$$a^2 + a^2 = 2a^2$$

is even, so $(a, a) \in R$.

Symmetric: Let $(a, b) \in R$. Then $a^2 + b^2$ is even. Since $b^2 + a^2 = a^2 + b^2$ is also even, $(b, a) \in R$.

Transitive: Let $(a, b), (b, c) \in R$. Then $a^2 + b^2 = 2k$ and $b^2 + c^2 = 2\ell$ for some integers k, ℓ .

Adding:

$$(a^2 + b^2) + (b^2 + c^2) = 2k + 2\ell = 2(k + \ell).$$

Thus

$$a^2 + c^2 = 2(k + \ell) - 2b^2 = 2(k + \ell - b^2),$$

which is even. Hence $(a, c) \in R$.

Therefore, R is reflexive, symmetric and transitive; thus R is an equivalence relation. \square

- (ii) **Equivalence classes.**

Note that $(a, b) \in R$ iff $a^2 + b^2$ is even, which holds iff a^2 and b^2 are both even or both odd, i.e. iff a and b are both even or both odd.

Thus:

- If a is even, then $[a] = \{n \in \mathbb{N} : n \text{ is even}\}$.
- If a is odd, then $[a] = \{n \in \mathbb{N} : n \text{ is odd}\}$.

There are exactly two equivalence classes:

$$[0] = \{\text{even natural numbers}\}, \quad [1] = \{\text{odd natural numbers}\}.$$

- (b) **Euclidean algorithm.**

$$224 = 126 \times 1 + 98,$$

$$126 = 98 \times 1 + 28,$$

$$98 = 28 \times 3 + 14,$$

$$28 = 14 \times 2 + 0.$$

The last nonzero remainder is 14.

Therefore,

$$\gcd(224, 126) = 14.$$

Mark Scheme:

- (a)(i) Clear verification of reflexivity, symmetry and transitivity of R using the condition “ $a^2 + b^2$ is even”. [6]
- (a)(ii) Explanation that R relates numbers exactly when they have the same parity, and description of the two resulting equivalence classes (even and odd naturals). [4]
- (b) Correct Euclidean algorithm steps leading to the last nonzero remainder 14, and conclusion that $\gcd(224, 126) = 14$. [5]