MATH1050BC/1058 Assignment 3

Advice.

1. The questions in this assignment are about integers, rational numbers and irrational numbers, divisibility, greatest common divisor, logical connectives, and formats of arguments of the type 'proof-by-contradiction', 'mathematical induction'. Do familiarize yourself with the corresponding material available in the course homepage before trying the questions.

2. (a) Questions (1)-(6) are about logical connectives.

   (b) Questions (7)-(18) are about integers, rational numbers and irrational numbers, divisibility, greatest common divisor.

   (c) Questions (19), (20) are mainly about the use of proof-by-contradiction arguments for conditional inequalities.

3. Questions which require more thought and/or work and/or tricks and/or organization and/or ... than the 'unlabelled' questions are labelled by $\diamondsuit, \clubsuit, \heartsuit, \spadesuit$ in ascending order of overall difficulty level.

Instructions.

1. Any work submitted by you must be written on **A4-size sheets** and must be appropriately binded.

   Your name and student ID, as in your student card, and the **code** of the section to which you are registered must be written at the upper right corner of the first page of your submission.

2. (a) **Mandatory work, for assessment purpose.**

   You are **required** to submit work on Questions (1), (3), (6), (7a), (7b.i), (8a), (8b.ii), (8c.i), (8c.ii), (9), (10), (11), (16), (17a), (17b.i) for course assessment purpose.

   (b) **Optional proof-writing exercise.**

   You may also **opt** to submit, **on exactly one sheet, separate from your submission on mandatory work**, your work on Questions (8c.iii), (19c). It will be read and commented, but not counted for course assessment.

   (c) **Other optional work.**

   You may choose to submit work on other questions in this assignment not mentioned above, alongside the mandatory work, but there is no guarantee that it will be read.

3. (a) You must adhere to the notations which have been inttroduced in the course. Things which have not been formally defined in the course are not allowed in your work.

   (b) When you are giving a proof for something, you must make it clear what you are assuming (and indicate your assumptions with the use of appropriate words at appropriate places). You are also expected to indicate the 'flow of logic' in the argument with correct and appropriate use of words/symbols.

   Be aware that the specific formats for arguments by 'mathematical induction', 'proof-by-contradiction' are dictated by mathematical reasons behind. A deviation from the appropriate formats may result in a mathematical mistake.

   (c) Many questions involve the use of '*there exist*' (the 'existential quantifier'). You must pay attention on: (a) when '*there exist*' should appear (or not) and how it should be used; (b) what it means by deducing something from a statement that involves '*there exist*'; (c) what it takes to deduce a statement that involves '*there exist*'.

   (d) Words of the likes of '*trivial*', '*obvious*', '*clear(-ly)*' are not allowed to appear in your work.

* * *

1. *In this question, you are not required to give any justification to your answers.*

   (a) Which of the statements below are true? Which are false?

   i. $2+3=6$ *or* $3+1=4$.
   ii. $2+3\leq 6$ *and* $(3+1\geq 4$ *or* $4+3<5)$.
   iii. *It is not true that* $(1+2>3$ *and* $3+4>2)$.
   iv. *If* $3+2\geq 5$ *then* $2+1\leq 3$.
   v. *If* $2+6\leq 5$ *then* $3+2=5$.
   vi. *If* $2+4\leq 3$ *then* $3+2=7$.
   vii. $2+3=6$ *iff* $1+4=7$.
   viii. *If* $[3+4=5$ *and* $($*if* $3+4=5$ *then* $2+3=4)]$ *then* $2+3=4$.

   (b) For each of the statements above, write down its negation in such a way that the word '*not*' (except in the context of the use of the symbol '$\neq$') does not appear explicitly.

2. Consider each of the compound statements formed with the atomic statements P, Q, R. Determine whether it is a tautology or a contradiction or a contingent statement . Justify your answer by drawing an appropriate truth table.

   (a) $(P \longrightarrow R) \longrightarrow [(P \longrightarrow Q) \wedge (Q \longrightarrow R)]$

(b) $(P \longrightarrow Q) \longrightarrow [(P \longrightarrow R) \vee (Q \longrightarrow R)]$

3. Denote by U, V, W, X the respective compound statements below, formed with the atomic statements P, Q:—

$$(P \longrightarrow Q) \longrightarrow Q, \qquad Q \longrightarrow (Q \longrightarrow P), \qquad (P \longrightarrow Q) \longrightarrow (\sim P), \qquad P \longrightarrow [Q \longrightarrow (\sim P)]$$

(a) Draw a truth table which displays the truth values of P, Q, U, V, W, X in all possible scenarios.

(b) Is U a tautology, or a contradiction, or a contingent statement?

(c) Is V a tautology, or a contradiction, or a contingent statement?

(d) Is W a tautology, or a contradiction, or a contingent statement?

(e) Is X a tautology, or a contradiction, or a contingent statement?

(f) Is $U \wedge V$ logically equivalent to P, or to Q, or to both, or to neither?

(g) Is $W \longleftrightarrow X$ a tautology, or a contradiction, or a contingent statement?

(h) Is $U \longleftrightarrow W$ logically equivalent to $P \longleftrightarrow Q$, or to $\sim(P \longleftrightarrow Q)$, or to neither?

4.$^{\diamondsuit}$ Let P, Q, R, S be statements, and denote the compound statements $(P \longrightarrow Q) \longrightarrow (R \longrightarrow S)$, $[P \longrightarrow (Q \longrightarrow R)] \longrightarrow S$ by U, V respectively.

Suppose the truth value of U is F. What is the truth value of $V \longrightarrow U$? Justify your answer. (It is of course possible to make use of a truth table. However, try to give an argument without using a truth table.)

5.$^{\diamondsuit}$ Let P, Q, R be statements. Determine whether $[(P \vee Q) \longrightarrow (Q \wedge R)] \longrightarrow (P \longrightarrow R)$ is a rule of inference. Justify your answer. (It is of course possible to make use of a truth table. However, try to give an argument without using a truth table.)

6. Let P, Q be statements. Denote by U the compound statement $[P \longrightarrow (\sim Q)] \wedge Q$.

(a) What is the truth value of U when the truth values of P, Q are both F?

(b) Is $U \longrightarrow (\sim P)$ a tautology, or a contradiction, or a contingent statement?

(c) Is $U \longrightarrow P$ a rule of inference?

7. (a) Fill in the blanks in the passage below so as to give the definition for the notion of *rational numbers*:

Suppose x is a real number. Then we say that x is **rational** *if* ____(I)____ *such that* ____(II)____ .

(b) Denote by (A), (B), (C), (D) the respective statements below:—

(A) *Let x, y be real numbers. Suppose x, y are rational. Then xy is rational.*

(B) *Let x, y be real numbers. Suppose x, y are rational. Then $x + y$ is rational.*

(C) *Let x, y be real numbers. Suppose x, y are rational. Then $x - y$ is rational.*

(D) *Let x, y be real numbers. Suppose x, y are rational and $y \neq 0$. Then $\dfrac{x}{y}$ is rational.*

i. Fill in the blanks (all labelled by capital-letter Roman numerals) in the *partially completed* proofs for the statements $(A), (B)$ in the corresponding blocks below, with appropriate words/symbols so as to obtain a *complete* proof for each respective statement.
(*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)
Here we prove the statement (A), with direct reference to the definition for rational numbers:—

> Let x, y be real numbers. Suppose x, y are rational.
>
> [We want to deduce that xy is rational.
> This amounts to verifying this statement: '____(I)____'.]
>
> By the definition of rational numbers, since x is a rational number, ____(II)____ $n \neq 0$ and $m = nx$.
> Also, since y is a rational number, there exist some integers p, q ____(III)____ .
> Note that $mp =$ ____(IV)____ .
> Since $n \neq 0$ and __(V)__ , we have __(VI)__ . Moreover, __(VII)__ , mp and __(VIII)__ are also integers.
> Hence, by the definition of rational numbers, ____(IX)____ .

Here we prove the statement (B), with direct reference to the definition for rational numbers:—

Let x, y be real numbers. _____(X)_____ .

[We want to deduce that $x + y$ is rational.
This amounts to verifying this statement: '_____(XI)_____'.]

By the definition of rational numbers, since x is a rational number, _____(XII)_____ .
Also, since y is a rational number, _____(XIII)_____ .
_____(XIV)_____
Hence, by the definition of rational numbers, _____(XV)_____ .

ii. Prove the statement (C), with direct reference to the definition for rational numbers.

iii. Prove the statement (D), with direct reference to the definition for rational numbers.

8. (a) i. Explain the word '*divisibility*' (for integers) by providing an appropriate definition.

ii. State the *Principle of Mathematical Induction*.

iii. State the *Well-ordering Principle for Integers*.

(b) Apply mathematical induction to prove (with direct reference to the definition of divisibility) the statements below:—

i. $n(n^2 + 2)$ *is divisible by* 3 *for any natural number* n.

ii. $2^{4n+3} + 3^{3n+1}$ *is divisible by* 11 *for any natural number* n.

iii.$^\diamondsuit$ $7^n(3n + 1) - 1$ *is divisible by* 9 *for any natural number* n.

(c) Prove the statements below (with direct reference to the definition of divisibility):

i. *Let* x, y *be integers. Suppose that* x *is divisible by* y*, and* y *is divisible by* x*. Then* $|x| = |y|$.

ii. *Let* x, y, z *be integers. Suppose that* x *is divisible by* y^2*, and* y *is divisible by* z^3*. Then* x *is divisible by* z^6.

iii.$^\diamondsuit$ *Let* x, n *be integers. Suppose that* x *is divisible by* n*. Then for any integer* y*, the integer* $(3x^2+4y)^5+(3x^2-4y)^5$ *is divisible by* $6n^2$.

9. (a) Prove the statement $(*)$, with direct reference to the definition of divisibility:—

$(*)$ *Let* x, y, a, b, d *be integers. Suppose that* x *is divisible by* d*, and* y *is divisible by* d*. Then* $ax + by$ *is divisible by* d.

(b) Denote by $(**)$ the statement below:—

$(**)$ *Let* n *be an integer greater than* 1*, and* $x_1, x_2, \cdots, x_n, a_1, a_2, \cdots, a_n, d$ *be integers. Suppose that* x_j *is divisible to by* d *for each* $j = 1, 2, \cdots, n$*. Then* $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ *is divisible by* d.

i. Fill in the blanks in the passage below so as to give a correct re-formulation $(**')$ for the statement $(**)$:

$(**')$ *Suppose* _____(I)_____ *. Then, for any integer* _____(II)_____ *, if* _____(III)_____ *are integers and* _____(IV)_____ *then* _____(V)_____ .

ii.$^\diamondsuit$ Apply mathematical induction to prove the statement $(**)$.

Remark. Your argument should take into account how $(**')$ reads. You may use $(*)$ in the argument.

10. (a) Explain the phrase '*prime number*' by stating the appropriate definition.

(b) With direct reference to the definition for prime numbers, prove the statement $(*)$:—

$(*)$ $n^2 + n - 6$ *is not a prime number for any integer* n *greater than* 3.

Remark. Can you formulate a conjecture on integers of the form '$n^2 + bn + c$' in which b, c are some 'fixed integers' and n is an arbitrary integer which may be as large as you like, and prove your conjecture (by generalizing your argument for $(*)$)?

11. (a) i. Explain the phrase '*common divisor*' (for integers) by stating the appropriate definition.

ii. State, without proof, *Euclid's Lemma* (on divisibility by prime numbers).

iii. State, without proof, *Division Algorithm for Natural Numbers*.

(b) Denote by (J), (K), (L) the respective statements below:—

(J) *Let* m *be an integer greater than* 1*, and* t, u, v *be real numbers. Suppose that* t *is non-zero and rational, and* u *is irrational, and* $v^m = tu$*. Then* v *is irrational.*

(K) *Let* a, p *be integers. Suppose* p *is a prime number. Then, for any integer* n *greater than* 1*, if* a^n *is divisible by* p *then* a *is divisible by* p.

(L) $\sqrt[5]{3}$ *is an irrational number.*

Fill in the blanks (all labelled by capital-letter Roman numerals) in the *partially completed* proofs for the statements $(J), (K), (L)$ in the corresponding blocks below, with appropriate words/symbols so as to obtain a *complete* proof for each respective statement.

(*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

i. Here we apply the proof-by-contradiction method to verify the statement (J):—

(I)

Further suppose that it were true that (II) .——(†)

By (†), v^m would also be (III) .

By assumption, $t \neq 0$. Then (IV) is well-defined as a real number, and the equality $u =$ (V) holds.

Since v^m, t were rational, (VI) . Also recall that by assumption, (VII) .

Then u would be simultaneously rational and irrational. Contradiction arises.

(VIII)

ii. Here we apply the method of mathematical induction and apply Euclid's Lemma to prove the statement (K):—

(I)

For each integer n greater than 1, denote by $Q(n)$ the proposition below:—

(II)

- [We verify $Q(2)$ is true.]

  (III)

  Then, by Euclid's Lemma, at least one of a, a is divisible by p. Therefore a is divisible by p.

  Hence $Q(2)$ is true.

- [We verify the statement '*for any integer k greater than* 1, *if $Q(k)$ is true then $Q(k+1)$ is true*'.]

  (IV)

  [We deduce $Q(k+1)$.]

  (V) . Note that $a^{k+1} = a \cdot a^k$.

  (VI) . If a^k is (VII) , then (VIII) .

  Therefore, (in any case,) a is divisible by p.

  Hence $Q(k+1)$ is true.

By the Principle of Mathematical Induction, $Q(n)$ is true for any integer n greater than 1.

iii. Here we apply the proof-by-contradiction method and apply the statement (K) to verify the statement (L):—

(I)

Then, by the definition of rational numbers, (II) .

Without loss of generality, we may assume that '$\sqrt[5]{3} = \dfrac{m}{n}$' is the lowest-term representation as a fraction of integers. Then (III) .

Since $m = n \cdot \sqrt[5]{3}$, the equality (IV) would hold.

Note that n^5 was an integer. Then, by the definition of divisibility, (V) .

Note that 3 is (VI) . Then, by the result described by the statement (K), (VII) .

Therefore, by the definition of divisibility, (VIII) .

Then we would have $3^5k^5 = (3k)^5 = m^5 = 3n^5$. Therefore $n^5 =$ (IX) .

Note that $3, k$ were integers. Then 3^3k^5 would also be (X) .

Therefore, by (XI) , n^5 would be (XII) .

Again by the result described by the statement (K), (XIII) .

Therefore simultaneously (XIV) , and 3 was a common divisor of (XV) .

Contradiction arises.

Therefore $\sqrt[5]{3}$ is an irrational number in the first place.

(c) By applying the results described in the previous part, or otherwise, prove the statements below.

i. *Each of* $\sqrt[5]{9}$, $\sqrt[5]{27}$, $\sqrt[5]{81}$ *is an irrational number.*

Remark. Can you express an appropriate positive integral power of, say, $\sqrt[5]{9}$, as the product of some non-zero rational number and $\sqrt[5]{3}$?

ii. *For any positive integer* m*, if* m *is not divisible by* 5 *then* $\sqrt[5]{3^m}$ *is an irrational number.*

Remark. Make use of the Division Algorithm for Natural Numbers.

12.$^\diamondsuit$ *In this question, take for granted that* $\sqrt{2}, \sqrt{3}$ are irrational numbers.

Apply proof-by-contradiction to justify the statements below:—

(a) $\sqrt{2}+\sqrt{3}$ *is an irrational number.*

Remark. Write $r = \sqrt{2}+\sqrt{3}$. Can you re-express one of $\sqrt{2}$, $\sqrt{3}$ as a fractional expression whose numerator and denominator involve only integers and the non-negative integral powers of r?

(b) $\sqrt{3}-\sqrt{2}$ *is an irrational number.*

Remark. See if you can generalize the argument to prove the statement (♯):—

(♯) *Suppose* a, b *are non-zero rational numbers, and* p, q *are distinct positive prime numbers. Then* $a\sqrt{p}+b\sqrt{q}$ *is an irrational number.*

13.$^\clubsuit$ Apply proof-by-contradiction to justify the statement (♯):—

(♯) $\sqrt{6}$ *is irrational.*

Remark. Take for granted the validity of Euclid's Lemma where appropriate and necessary. You may also take for granted the validity of statements like '2 *is not divisible by* 3', '3 *is not divisible by* 2'.

Further remark. Can you generalize the argument for statement (♯) to give a proof for the statement (♯′) below? Or even the statement (♯″)?

(♯′) *Suppose* p, q *are distinct positive prime numbers. Then* $\sqrt{pq}$ *is irrational.*

(♯″) *Suppose* p, q *are distinct positive prime numbers, and* n *is an integer greater than* 1*. Then* $\sqrt[n]{pq}$ *is irrational.*

14. (a) With direct reference to the definition of prime numbers, prove the statement (♯):—

(♯) *Let* p, q *be positive integers. Suppose* p, q *are prime numbers, and* q *is divisible by* p*. Then* $p = q$*.*

(b) Hence, or otherwise, prove the statement (♮):—

(♮) *Suppose* p, q *are distinct positive prime numbers, and* m, n *are positive integers. Then* $p^m - q^n$ *is divisible by neither* p *nor* q*.*

Remark. You may take for granted the validity of Euclid's Lemma (or its generalization to the 'many-numbers situation'.)

15. (a)$^\clubsuit$ Applying the Division Algorithm for Natural Numbers, or otherwise, prove the statement (♮):—

(♮) *Suppose* n *is a positive integer. Then, for any natural number* x*, exactly one of* $x, x+1, x+2, \cdots, x+n-1$ *is divisible by* n*.*

Remark. Be aware that '*exactly one of blah-blah-blah*' contains more 'information' than '*(at least) one of blah-blah-blah*'. It should be understood as '*at least one, and at most one, of blah-blah-blah*'.

(b) Suppose p is a prime number and $p \geq 5$.

i.$^\diamondsuit$ Applying the result above, or otherwise, verify the statement (∗):—

(∗) p^2-1 *is divisible by* 8 *and* p^2-1 *is divisible by* 3.

ii.$^\clubsuit$ Hence, or otherwise, and applying Euclid's Lemma (if necessary), verify the statement (∗∗):—

(∗∗) p^2-1 *is divisible by* 24.

Remark. Can you conjecture a result analogous to the above for the numbers of the form '$(p^2-1)(p^2-4)$' in which p is an arbitrary positive prime number greater than 5?

16. (a) Fill in the blanks in the passage below so as to give the definition for the notion of *greatest common divisor* (for integers):

Let m, n *be integers. If* $m = n = 0$*, then we declare the greatest common divisor of* m, n *is* 0*.*
From now on suppose m, n *are not both zero. Suppose* g *is a natural number.*
Then we say that g *is a* **greatest common divisor of** m, n *if both of the statements* (1), (2) *hold:—*

(1) g *is* _____(I)_____

(2) __(II)__ d, _____(III)_____ .

(b) i. With direct reference to the definition for the notion of greatest common divisor, determine $\gcd(120, 75)$.

ii. Apply Euclidean Algorithm to determine $\gcd(120, 75)$.

(c)$^{\diamondsuit}$ Let n be a positive integer. Apply Euclidean Algorithm to determine $\gcd\left(\sum_{j=0}^{23} n^j, \sum_{j=0}^{14} n^j\right)$.

17. (a) State, without proof, *Bézout's Lemma* (for integers).

(b)$^{\diamondsuit}$ By applying Bézout's Lemma, or otherwise, prove the statements below:—

i. *Let x,y,z be integers. Suppose* $\gcd(y, z)=1$. *Further suppose that xy is divisible by z. Then x is divisible by z.*
Remark. The key to the argument is to obtain an equality about integers only, with x being alone on one side and z being a 'factor' in a product on the other side. Bézout's Lemma 'supplies the key ingredients' for such an equality.

ii. *Let x, y, z be integers. Suppose* $\gcd(y, z) = 1$. *Further suppose that x is divisible by y and x is divisible by z. Then x is divisible by yz.*

(c) i.$^{\diamondsuit}$ With direct reference to the definition for the notion of greatest common divisor, prove the statement ($\natural$):—

($\natural$) *Suppose a, b be integers. Then the statements ($\natural_1$), ($\natural_2$) are logically equivalent:—*

($\natural_1$) $\gcd(a, b) = 1$.

($\natural_2$) *There exist some integers s, t such that $sa + tb = 1$.*

ii.$^{\diamondsuit}$ Hence, or otherwise, prove the statement below:—

($\flat$) *Let x, y, z be integers. Suppose* $\gcd(x, y) = 1$ *and* $\gcd(x, z) = 1$. *Then* $\gcd(x, yz) = 1$.

18. (a)$^{\clubsuit}$ Applying the Division Algorithm for Natural Numbers, or otherwise, prove the statement ($\sharp$) (which can be called the 'Division Algorithm for Integers with positive divisor'):—

($\sharp$) *Let u, n be integers. Suppose $n > 0$. Then there exist some unique integers q, r such that $u = qn + r$ and $0 \leq r < n$.*

(b)$^{\heartsuit}$ Applying the statement ($\sharp$) and Bézout's Lemma, or otherwise, prove the statement ($\star$):—

($\star$) *Let x, y, p be integers. Suppose p is a positive prime number, and x is not divisible by p, and $0 < y < p$. Then there exists some unique integer s such that $0 < s < p$ and $sx - y$ is divisible by p.*

Remark. The 'existence part' and the 'uniqueness part' had better be taken care of separately.

19. For each statement below, give an argument with the proof-by-contradiction method.

(a) *Let a, b be complex numbers. Suppose $a^4 + a^3b + a^2b^2 + ab^3 + b^4 \neq 0$. Then at least one of a, b is non-zero.*

(b) *Let a be a real number and b be a complex number. Suppose $a^3|b| > 2$. Then $a^6 + 9|b|^2 > 6$.*

(c)$^{\diamondsuit}$ *Let ζ be a complex number. Suppose that for any positive real number ε, the inequality $|\zeta| \leq \varepsilon$ holds. Then $\zeta = 0$.*

(d)$^{\clubsuit}$ *Let a, b be real numbers. Suppose $a > b > 0$. Then $\sqrt{a^2 - b^2} + \sqrt{2ab - b^2} > a$.*

20. For each positive integer n, define $A_n = \sum_{j=1}^{n} \frac{1}{j}$, $B_n = \sum_{k=1}^{n} \frac{1}{2k}$, $C_n = \sum_{k=1}^{n} \frac{1}{2k-1}$.

(a) i. Prove that $B_n = \frac{1}{2}A_n$ and $C_n = A_{2n} - \frac{1}{2}A_n$ for any positive integer n.

ii.$^{\diamondsuit}$ Prove that $C_n - B_n \geq \frac{1}{2}$ for any integer n greater than 1.

(b)$^{\clubsuit}$ By applying the proof-by-contradiction method, or otherwise, prove that $\{A_n\}_{n=1}^{\infty}$ does not converge in $\mathbb{R}$.

Remark. Take for granted the results ($\star$), ($\star\star$) about inequality for limits of infinite sequences:—

($\star$) *Let $\{u_n\}_{n=0}^{\infty}$ be an infinite sequence of real numbers. Suppose $\{u_n\}_{n=0}^{\infty}$ converges to some real number, say, v. Then $\{u_{pn}\}_{n=0}^{\infty}$ converges to v for each integer p greater than 1.*

($\star\star$) *Let $\{x_n\}_{n=0}^{\infty}$ be an infinite sequence of real numbers, and t be a real number. Suppose $x_n \geq t$ for any $n \in \mathbb{N}$. Also suppose $\{x_n\}_{n=0}^{\infty}$ converges in $\mathbb{R}$. Then $\lim_{n\to\infty} x_n \geq t$.*