MATH1050 Exercise 7

1. Consider each of the statements below. (Do not worry about the mathematical content.) Write down its negation in such a way that the word '*not*' does not explicitly appear.

   (a) *For any $x \in \mathbb{R}$, there exist some $s, t \in \mathbb{Q}$ such that for any $n \in \mathbb{Z}$, if $s < n < t$ then $|x - n| > |t - s|$.*

   (b) *For any $p \in \mathbb{R}$, there exists some $q \in \mathbb{R}$, $n \in \mathbb{N}$ such that for any $s, t \in \mathbb{R}$, if $|s - t| < |q|$ then $|s^n - t^n| < |p|$.*

   (c) *For any $s, t \in \mathbb{Q}$, there exist some $p, q \in \mathbb{R}$ such that for any $n \in \mathbb{Z}$, (if $|s - t| \leq |q|$ then ($t^n \leq |p|$ and $s^n \leq |p|$)).*

   (d) *There exists some $n \in \mathbb{N}$ such that (for any $\varepsilon \in (0, +\infty)$, there exists some $\delta \in (0, +\infty)$ such that (for any $u, v \in \mathbb{C}$, if $|u - v| < \delta$ then $|u^n - v^n| < \varepsilon$)).*

   (e) *For any $p, q \in \mathbb{Z}$, there exist some $s, t \in \mathbb{Z}$ such that for any $m, n \in \mathbb{N}$, if $|p + q| \geq s^m$ then ($|p^n - q| < t$ or $|p - q^n| < t$).*

   (f) *For any $z \in \mathbb{C}$, there exists some $r \in \mathbb{R}$ such that for any $w \in \mathbb{C}$, (if $|z - w| \leq r$ then ($z \notin \mathbb{R}$ and $|w| > r$)).*

   (g) *For any $z, w \in \mathbb{C}$, if $|z - w| \geq |z + w|$ then (there exists some $s \in \mathbb{R}$ such that (for any $t \in \mathbb{R}$, ($|z - s - t| > |w|$ or $|z| < 1$))).*

   (h) *For any $\zeta, \alpha, \beta \in \mathbb{C}$, if (there exist some $s, t \in \mathbb{R}$ such that $\zeta = s\alpha + t\beta$) then (there exist some $p, q \in \mathbb{R}$ such that $\zeta = p\bar{\alpha} + q\bar{\beta}$).*

2. Prove each of the 'existence statements' below.

   (a) *There exists some $n \in \mathbb{N}$ such that $n, n + 2, n + 4$ are prime numbers.*

   Remark. The proof is easy. Do not think too hard.

   (b) *There exists some $x \in \mathbb{R}$ such that $x^2 - 2 = 0$.*

   (c) *There exists some $z \in \mathbb{C}$ such that $z^4 = -1$.*

3. (a) Prove each of the statements below:

   i. *There exists some $x \in \mathbb{Z}$ such that $x + 1 < 0$.*
   ii. *There exists some $x \in \mathbb{Z}$ such that $x - 1 > 0$.*

   (b) Dis-prove the statement below:

   - *There exists some $x \in \mathbb{Z}$ such that ($x + 1 < 0$ and $x - 1 > 0$).*

   Remark. It can happen that $[(\exists x)P(x)] \wedge [(\exists y)Q(y)]$ is true while $(\exists x)(P(x) \wedge Q(x))$ is false. In general, $[(\exists x)P(x)] \wedge [(\exists y)Q(y)]$ does not imply $(\exists x)(P(x) \wedge Q(x))$.

4. (a) Prove the statement below:

   - *For any $z \in \mathbb{C} \backslash \{0\}$, ($\mathsf{Re}(z) \neq 0$ or $\mathsf{Im}(z) \neq 0$).*

   (b) Dis-prove the statement below:

   - *(For any $z \in \mathbb{C} \backslash \{0\}$, $\mathsf{Re}(z) \neq 0$) or (for any $w \in \mathbb{C} \backslash \{0\}$, $\mathsf{Im}(w) \neq 0$).*

   Remark. It can happen that $(\forall x)(P(x) \vee Q(x))$ is true and $[(\forall x)P(x)] \vee [(\forall y)Q(y)]$ is false. In general, $(\forall x)(P(x) \vee Q(x))$ does not imply $[(\forall x)P(x)] \vee [(\forall y)Q(y)]$.

5. (a) Consider the statement (A):

   (A) *Let $\zeta \in \mathbb{C} \backslash \mathbb{R}$. For any $\eta \in \mathbb{C}$, there is at most one $a \in \mathbb{R}$ and at most one $b \in \mathbb{R}$ satisfying $\eta = a\zeta + b\zeta^2$.*

   Fill in the blanks in the block below, all labelled by capital-letter Roman numerals, with appropriate words so that it gives a proof for the uniqueness statement (A). (*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

Let $\zeta \in \mathbb{C} \backslash \mathbb{R}$. Let $\eta \in \mathbb{C}$, and $a, a', b, b' \in \mathbb{R}$.
$\underline{\quad\text{(I)}\quad}$ $\eta = a\zeta + b\zeta^2$ and $\underline{\qquad\text{(II)}\qquad}$.
Then $a\zeta + b\zeta^2 = a'\zeta + b'\zeta^2$.
Since $\zeta \notin \mathbb{R}$, we have $\underline{\quad\text{(III)}\quad}$ in particular. Then $a + b\zeta = a' + b'\zeta$.
Therefore $(b - b')\zeta = \underline{\quad\text{(IV)}\quad}$.
We claim that $b = b'$. We justify this claim with a proof-by-contradiction argument:

* $\underline{\qquad\qquad\text{(V)}\qquad\qquad}$.

  Then $b - b' \neq 0$. Therefore $\zeta = \underline{\quad\text{(VI)}\quad}$.

  Since a, a', b, b' are real, ζ would be real. Contradiction arises.

Now we have verified that $b = b'$. Then $a' - a = (b - b')\zeta = 0$. Therefore $\underline{\quad\text{(VII)}\quad}$ also.

(b) Prove each of the statements below.

i. *Let r be a real number. There is at most one rational number a and at most one rational number b satisfying $r = a + b\sqrt{2}$.*

ii. *Let p, q be real numbers. Suppose $f(x)$ be the cubic polynomial given by $f(x) = x^3 + px + q$. Then, for each real number v, the equation $f(u) = v$ with unknown u has at most one real solution.*

6. (a) Consider the statement (B):

(B) *Let $x, y, z \in \mathbb{Z}$. Suppose each of xy, xz is divisible by 4. Then xyz is divisible by 8.*

Fill in the blanks in the block below, all labelled by capital-letter Roman numerals, with appropriate words so that it gives a dis-proof against the statement (B). (*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

The negation of the statement (B) reads:

- $\underline{\qquad\qquad\qquad\text{(I)}\qquad\qquad\qquad}$

We verify the negation of the statement (B) below:

- Take $x = 4$, $\underline{\qquad\text{(II)}\qquad}$. We have $x, y, z \in \mathbb{Z}$.

  Note that $xy = \underline{\quad\text{(III)}\quad}$, and $xz = \underline{\quad\text{(IV)}\quad}$.

  Note that $\underline{\qquad\qquad\text{(V)}\qquad\qquad}$. Then xy is divisible by 4.

  By a similar argument, we also deduce that xz is divisible by 4.

  Note that $xyz = \underline{\quad\text{(VI)}\quad}$, which is not divisible by 8.

  Below is the justification of this claim:

  * Suppose it were true that $\underline{\qquad\qquad\text{(VII)}\qquad\qquad}$.

    Then there would exist some $k \in \mathbb{Z}$ such that $\underline{\qquad\text{(VIII)}\qquad}$.

    For the same k, we would have $k = \underline{\quad\text{(IX)}\quad}$, which is not an integer. Contradiction arises.

(b) Dis-prove each of the statements below. (It may help if you first find what the negation of the statement is.)

i. *Let $x, y, z \in \mathbb{N}$. Suppose $x + y$, $y + z$ are divisible by 3. Then $x + z$ is divisible by 3.*

ii. *Let $x, y, z \in \mathbb{N}$. Suppose $x - y > 0$ and $x - z > 0$ and $x - z$, $y - z$ are divisible by 5. Then $x + y + z$ is not divisible by 5.*

iii. *Suppose $x, y \in \mathbb{N}$. Then $\sqrt{x^2 + y^2} \in \mathbb{N}$.*

iv.$^\diamondsuit$ *For any $s, t \in \mathbb{R}$, if both of $s + t, st$ are rational, then at least one of s, t is rational.*

v.$^\diamondsuit$ *For any $a, b, c \in \mathbb{N}$, if ab is divisible by c and $c < a$ and $c < b$, then at least one of a, b is divisible by c.*

7. (a) Consider the statement (C):

   - *There exist some* $u \in \mathbb{R} \backslash \{-1, 0, 1\}$, $v \in \mathbb{R}$ *such that* $u^2 + v^2 \leq 2u^4$ *and* $u^6 + v^6 \leq 2v^4$.

   Fill in the blanks in the block below, all labelled by capital-letter Roman numerals, with appropriate words so that it gives a dis-proof against the statement (C). (*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

   > (We dis-prove the statement (C) by obtaining a contradiction from it.)
   > __(I)__ there existed some __(II)__, $v \in \mathbb{R}$ such that $u^2 + v^2 \leq 2u^4$ and __(III)__.
   > For the same u, v, we would have $u^2 + v^2 - 2u^4 \leq 0$ and $u^6 + v^6 - 2v^4 \leq 0$.
   > Then $u^2(u^2 - 1)^2 + v^2(v^2 - 1)^2 =$ __(IV)__.
   > Since u, v are real, $u^2(u^2 - 1)^2 \geq 0$ and $v^2(v^2 - 1)^2 \geq 0$. Then $u^2(u^2 - 1)^2 = 0$ and $v^2(v^2 - 1)^2 = 0$ respectively.
   > In particular, __(V)__. Then $u = 0$ or $u = -1$ or $u = 1$. But __(VI)__.
   > Contradiction arises.

   (b) Dis-prove each of the statements below. (Note that each of them is an 'existence statement'.)

   i. *There exists some* $x \in \mathbb{R}$ *such that* $x^2 + 2x + 3 < 0$.
   ii. *There exist some* $x, y \in \mathbb{R} \backslash \{0\}$ *such that* $(x + y)^2 = x^2 + y^2$.
   iii. *There exists some* $x \in \mathbb{R}$ *such that* $|x + 1| > |x| + 1$.
   iv.$^\diamond$ *There exists some* $z \in \mathbb{C}$ *such that* $|z + 3 - 4i| > |z| + 5$.
   v.$^\diamond$ *There exists some* $x \in \mathbb{R}$ *such that* $|x + 4| > 2|x + 1| + |x - 2|$.

8. (a) Let $s \in \mathbb{Z}$. Apply the Division Algorithm for integers to prove that the statements $(\dagger), (\ddagger)$ are logically equivalent:

   $(\dagger)$ *s is not divisible by* 2.
   $(\ddagger)$ *There exists some* $k \in \mathbb{Z}$ *such that* $s = 2k + 1$.

   Remark. Hence it makes to use any one of $(\dagger)$, $(\ddagger)$ to define **odd-ness** for integers, leaving the other as a consequence of the definition.

   (b) Prove the statements below:

   - *Let* $a, b \in \mathbb{Z}$. *ab is an odd integer iff both of* a, b *are odd integers.*

9. Let $f(x)$ be the polynomial given by $f(x) = x^7 + 3x^3 + 5$ with indeterminate x.

   (a) Let $p \in \mathbb{Z}$ and $q \in \mathbb{Z} \backslash \{0\}$. Suppose p, q have no common divisors. Prove that $q^7 f\left(\frac{p}{q}\right)$ is an odd integer.

   (b) Hence, or otherwise, prove that no root of the polynomial $f(x)$ is a rational number.

10.$^\clubsuit$ Let p, m, n be positive integers. Suppose $p > 1$ and $m > n > 1$. Suppose r is the remainder in division of m by n. Prove that the remainder in the division of $\dfrac{p^m - 1}{p - 1}$ by $\dfrac{p^n - 1}{p - 1}$ is $\dfrac{p^r - 1}{p - 1}$.

    Remark. It looks obvious that the result is a consequence of Division Algorithm. The question is: how do you apply it in the argument?

11. Consider each of the pairs of integers below. Apply the Euclidean Algorithm to find their greatest common divisor.

    (a) $14, 35$
    (b) $11, 15$
    (c) $180, 252$
    (d) $1368, 1278$

12. (a)$^\diamond$ Apply the Euclidean Algorithm to prove the statements below:

    i. *Let* $n \in \mathbb{N} \backslash \{0, 1\}$. $\gcd(n, n + 1) = 1$.
    ii. *Let* $n \in \mathbb{N} \backslash \{0, 1\}$. $\gcd(2n - 1, 2n + 1) = 1$.

(b)$^\clubsuit$ Conjecture what can be said about $\gcd(3n-1, 3n+1)$ for each $n \in \mathbb{N}\backslash\{0,1\}$. Formulate your conjecture appropriately as a mathematical statement.
Prove your conjecture.

13. Let p be a positive prime number. Prove the statements below:

(a)$^\clubsuit$ *For any* $r \in [\![1, p-1]\!]$, $\left(\begin{array}{c} p \\ r \end{array}\right)$ *is divisible by* p.

(b) *For any* $x, y \in \mathbb{Z}$, $(x+y)^p \equiv x^p + y^p (\mathsf{mod}\ p)$.

(c)$^\diamondsuit$ *For any* $x \in \mathbb{N}\backslash\{0\}$, $x^p \equiv x (\mathsf{mod}\ p)$.

(d)$^\clubsuit$ *For any* $x \in \mathbb{Z}$, $x^p \equiv x (\mathsf{mod}\ p)$.

Remark. In part (a), you may need Euclid's Lemma at some stage of the argument. In part (b), apply the Binomial Theorem. In part (c), apply mathematical induction. The statement in part (d) is a 'generalization' of the result in part (c), and is known as **Fermat's Little Theorem**. To prove it, make good use of part (c) where applicable.

14. Dis-prove each of the statements below by giving an appropriate argument. (It may help if you draw Venn diagrams to investigate the respective statements first.)

(a) *Let* A, B, C *be sets.* $A\backslash(C\backslash B) \subset A \cap B$.

(b) *Let* A, B, C *be non-empty sets.* $B\backslash A \subset (C\backslash A)\backslash(C\backslash B)$.

(c) *Let* A, B, C *be non-empty sets.* $A \cup (B \cap C) \subset (A \cup B) \cap C$.

(d)$^\diamondsuit$ *Let* A, B, C *are non-empty sets.* $B \cap C \subset [A\backslash(B\backslash C)] \cup [B\backslash(C\backslash A)]$.

(e)$^\diamondsuit$ *Let* A, B, C *be sets. Suppose* $A \cap B \subset C$*. Then* $C \subset (A \cap C) \cup (B \cap C)$.

(f)$^\diamondsuit$ *Let* A, B, C *be sets. Suppose* $A\backslash B$, $A\backslash C$ *are non-empty. Then* $A\backslash(B \cap C) \subset (A\backslash B) \cap (A\backslash C)$.

(g)$^\diamondsuit$ *Let* A, B, C, D *be non-empty sets. Suppose* $A \subset C$ *and* $B \subset D$*. Further suppose* $C \cap D \neq \emptyset$*. Then* $A \cup B \subset C \cap D$.

15. We introduce the definition below:

- *Let* A, B *be sets.* A *is said to be a* **proper subset** *of* B *if* $A \subset B$ *and* $A \neq B$*. We write* $A \subsetneqq B$.

Prove the statements below:

(a) *Let* A, B *be sets. Then* $A \subsetneqq B$ *iff* ($A \subset B$ *and* $B \not\subset A$).

(b) *Let* A, B, C *be sets. Suppose* $A \subset B$ *and* $B \subset C$*. Further suppose* $A \subsetneqq B$ *or* $B \subsetneqq C$*. Then* $A \subsetneqq C$.

16. (a) Prove the statements below 'from first principles', using the definitions of set equality, subset relation, intersection, union, complement, where appropriate.

i. *Let* E *be a set, and* A, B *be subsets of* E*. Suppose* $A \subset B$*. Then* $E\backslash B \subset E\backslash A$.

ii. *Let* E *be a set, and* A, B *be subsets of* E*. Suppose* $A \subsetneqq B$*. Then* $E\backslash B \subsetneqq E\backslash A$.

(b) Consider each of the statements below. For each of them, determine whether it is true or false. Justify your answer by giving a proof or constructing a counter-example where appropriate.

i. *Let* A, B, E *be a set. Suppose* $A \subset B$*. Then* $E\backslash B \subset E\backslash A$.

ii. *Let* A, B, E *be a set. Suppose* $A \subsetneqq B$*. Then* $E\backslash B \subsetneqq E\backslash A$.

17. Let M be a set, and C be a subset of $\mathfrak{P}(M)$.
Define $I = \{x \in M : x \in V \text{ for any } V \in C\}$, $J = \{x \in M : x \in V \text{ for some } V \in C\}$.
Prove the statements below:

(a)$^\diamondsuit$ *Let* P *be a subset of* M*. Suppose* $P \subset V$ *for any* $V \in C$*. Then* $P \subset I$.

(b)$^\diamondsuit$ *Let* Q *be a subset of* M*. Suppose* $V \subset Q$ *for any* $V \in C$*. Then* $J \subset Q$.

(c)$^\clubsuit$ *Let* R *be a subset of* M*. Suppose* $D = \{V \cap R \mid V \in C\}$*, and* $K = \{x \in M : x \in U$ *for some* $U \in D\}$*. Then* $K = J \cap R$.