MATH1050 Assignment 6

1. *This is a review question on the framework of proofs of statements starting with* there exists.

   Prove each of the 'existence statements' below. (The proofs are easy: conceive the candidates and verify the candidacy. Do not think too hard.)

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

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

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

2. 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 (A), a dis-proof against the statement (B), a dis-proof against the statement (C) and a dis-proof against the statement (D). (*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

   (a) We dis-prove the statement (A):

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

   [The negation of the statement (A) is given by:

   $(\sim A)$ _____ (I) _____]

   - We verify the negation of the statement (A) below:

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

     Note that $xy =$ _____ (III) _____ , and $xz =$ _____ (IV) _____ .

     Note that _____ (V) _____ . Then xy is divisible by 4.

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

     Note that $xyz =$ _____ (VI) _____ , which is not divisible by 8.

     Below is the justification of this claim:

     * Suppose it were true that _____ (VII) _____ .

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

       For the same k, we would have $k =$ _____ (IX) _____ , which is not an integer. Contradiction arises.

   (b) We dis-prove the statement (B):

   (B) *Let* A, B, C *be sets. Suppose* $A \cap B \neq \emptyset$ *and* $A \cap B \subset C$. *Then* $A \subset C$ *or* $B \subset C$.

   [The negation of the statement (B) is given by:

   $(\sim B)$ _____ (I) _____]

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

   - Take $A = \{1, 3\}$, $B = \{2, 3\}$ and _____ (II) _____ .

     We have $A \cap B = \{3\}$. Then $A \cap B \neq$ _____ (III) _____ .

     Moreover $A \cap B = C$. Then _____ (IV) _____ .

     We verify $A \not\subset C$ and $B \not\subset C$:

     * We have $1 \in A$ _____ (V) _____ . Then _____ (VI) _____ .

       We have _____ (VII) _____ . Then _____ (VIII) _____ .

       Hence $A \not\subset C$ and $B \not\subset C$ (simultaneously).

(c) We dis-prove the statement (C):

(C) *Let $x, y \in \mathbb{R}$. Suppose $x > 0$ and $y > 0$ and $|x^2 - 2x| < |y^2 - 2y|$. Then $x^2 \leq y^2$.*

> [The negation of the statement (C) is given by:
>
> $(\sim C)$ _____(I)_____]
>
> We verify the negation of the statement (C) below:
>
> - Take $x = 2$, ____(II)____ . We have $x, y \in \mathbb{R}$, and _____(III)_____ .
>
> Note that $|x^2 - 2x| =$ ____(IV)____ and _____(V)_____ . Then ____(VI)____ < ____(VII)____ .
>
> We have ____(VIII)____ and $y^2 = 1$. Then ____(IX)____ .

(d) We dis-prove the statement (D):

(D) *Let $m, n \in \mathbb{N}\backslash\{0, 1, 2\}$ and $\zeta, \omega \in \mathbb{C}$. Suppose $m \neq n$, $\zeta \neq \omega$, ζ is an m-th root of unity and ω is an n-th root of unity. Then $\zeta\omega$ is an $(m + n)$-th root of unity.*

> [The negation of the statement (D) is given by:
>
> $(\sim D)$ _____(I)_____]
>
> We verify the negation of the statement (D) below:
>
> - ____(II)____ $m = 4$, $n = 8$, $\zeta = i$ and _____(III)_____ .
>
> We have $m, n \in \mathbb{N}\backslash\{0, 1, 2\}$ and $\zeta, \omega \in \mathbb{C}$. Also, _____(IV)_____ .
>
> Note that $\zeta^m = i^4 = 1$. Then _____(V)_____ .
>
> Note that _____(VI)_____ . Then ω is an n-th root of unity.
>
> Now note that $m + n =$ ____(VII)____ and $\zeta\omega = \cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right)$.
>
> We have _____(VIII)_____ . Then $(\zeta\omega)^{m+n}$ ____(IX)____ 1.
>
> Therefore _____(X)_____ .

3. (a) Prove the statement $(\sharp)$:

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

(b) Dis-prove the statement $(\flat)$:

$(\flat)$ *(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 $(\forall x)[H(x) \to (P(x) \vee Q(x))]$ is true and $[(\forall x)(H(x) \to P(x))] \vee [(\forall y)(H(y) \to Q(y))]$ is false. In general, $(\forall x)[H(x) \to (P(x) \vee Q(x))]$ does not imply $[(\forall x)(H(x) \to P(x))] \vee [(\forall y)(H(y) \to Q(y))]$.

4. (a) Recall how **evenness**, **oddness** for integers is defined:

- *Suppose n is an integer. Then n is said to be even if n is divisible by 2.*
- *Suppose m is an integer. Then m is said to be odd if m is not even.*

Also recall the result known as the **Division Algorithm for integers**:

Suppose $u, v \in \mathbb{Z}$, and $v > 0$. Then there exist some unique $q, r \in \mathbb{Z}$ such that $u = qv + r$ and $0 \leq v < r$.

Consider the statement (G):

(G) *Suppose s is an integer. Then the statement $(\dagger), (\ddagger)$ are logically equivalent:*

$(\dagger)$ *s is not divisible by 2.*

$(\ddagger)$ *there exists some $k \in \mathbb{Z}$ such that $s = 2k + 1$.*

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 statement (G) with the help of the Division Algorithm for integers. (*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

(In the light of the validity of the statement (G), it makes sense to define **odd-ness** for integers through any one of $(\dagger), (\ddagger)$, leaving the other as a consequence of the definition.)

(I) s is an integer.

- [We want to prove that *if s is not divisible by 2 then there exists some $k \in \mathbb{Z}$ such that $s = 2k + 1$.*]

  (II)

  By the Division Algorithm for Integers, (III) .

  Since (IV) , we have $r \neq 0$. Then (V) . Now, since $0 < r < 2$ and (VI) , we have $r = 1$.

  Hence (VII) for the same $k \in \mathbb{Z}$.

- [We want to prove that (VIII) .]

  Suppose there exists some $k \in \mathbb{Z}$ such that $s = 2k + 1$.

  We verify with the help of the proof-by-contradiction argument that s is not divisible by 2:

  * (IX)

    Then (X) .

    Now we would have $k, \ell \in \mathbb{Z}$ and (XI) . Note that $0 \leq 0 < 2$ and $0 \leq 1 < 2$.

    (XII) , we would have $k = \ell$ and $0 = 1$. In particular, (XIII) .

    Contradiction arises.

    Hence s is not divisible by 2 in the first place.

(b) Prove the statement (♯) below:

(♯) *Suppose a, b are integers. Then ab is an odd integer iff both of a, b are odd integers.*

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

i. *Let $p \in \mathbb{Z}$ and $q \in \mathbb{Z}\backslash\{0\}$. Suppose p, q have no common divisors other than $1, -1$. Then $q^7 f\left(\frac{p}{q}\right)$ is an odd integer.*

ii. *No root of the polynomial $f(x)$ is a rational number.*

5. (a)$^\diamondsuit$ Apply Division Algorithm to prove the statement (♯):

(♯) *Suppose $n \in \mathbb{N}\backslash\{0, 1\}$. Then, for any $x \in \mathbb{Z}$, exactly one of $x, x + 1, x + 2, \cdots, x + n - 1$ is divisible by n.*

(b) Let $p \in \mathbb{N}$. Suppose p is a prime number and $p \geq 5$. Prove the statements below. *Where appropriate and necessary, you may apply Euclid's Lemma.*

i. *$p^2 - 1$ is divisible by 8.* ii.$^\diamondsuit$ *$p^2 - 1$ is divisible by 3.* iii.$^\clubsuit$ *$p^2 - 1$ is divisible by 24.*

6.$^\diamondsuit$ Let n be a positive integer. Apply Euclidean Algorithm to determine the greatest common divisor of $n^7 + n^6 + n^5 + n^4 + n^3 + n^2 + n + 1$ and $n^4 + n^3 + n^2 + n + 1$. Justify your answer.

7. Prove the statement (⋆) below:

(⋆) *Let $m \in \mathbb{N}$ and $m \geq 2$. Suppose that for any $a, b \in \mathbb{Z}$, if ab is divisible by m then at least one of a, b is divisible by m. Then m is a prime number.*

Remark. Combining the statement (⋆) with Euclid's Lemma, we obtain this characterization of prime numbers:

Suppose $p \in \mathbb{Z}\backslash\{-1, 0, 1\}$. Then the statements (†), (‡) are logically equivalent:

(†) *p is a prime number.*

(‡) *For any $a, b \in \mathbb{Z}$, if ab is divisible by p then at least one of a, b is divisible by p).*

8.$^\diamondsuit$ We introduce the definition for the notion of *being relatively prime* below:

- *Suppose a, b are integers. Then a, b are said to be* **relatively prime** *if* $\gcd(a, b) = 1$.

Also recall the result known as the **Bézout's Identity**:

Suppose m, n are integers. Then there exist some $s, t \in \mathbb{Z}$ such that $sm + tn = \gcd(m, n)$.

(a) Consider the statement (K):

(K) *Let a, b, c be integers. Suppose a, c are relatively prime and ab is divisible by c. Then b is divisible by c.*

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 statement (K) with the help of Bézout's Identity. (*The 'underline' for each blank bears no definite relation with the length of the answer for that blank.*)

> Let a, b, c be integers. ____(I)____ .
> Since __(II)__ , there exists some __(III)__ such that $ab = kc$.
> Since a, c are relatively prime, we have __(IV)__ . —— $(\star)$
> By Bézout' Identity, __(V)__ such that $\gcd(a, c) =$ __(VI)__. —— $(\star\star)$
> By $(\star), (\star\star)$, we have $1 =$ __(VII)__ $= sa + tc$.
> Now we have $b = 1 \cdot b =$ __(VIII)__.
> Note that b, k, s, t are integers. Then __(IX)__ is also an integer.
> Therefore __(X)__ .

(b) Prove each of the statements below without applying the Fundamental Theorem of Arithmetic. Where necessary and appropriate, you may apply Bézout's Identity.

i. *Let $a, b \in \mathbb{Z}$. Suppose there exist some $s, t \in \mathbb{Z}$ such that $sa + tb = 1$. Then a, b are relatively prime.*
Remark. It follows that a, b are relatively prime iff there exist some $s, t \in \mathbb{Z}$ such that $sa + tb = 1$. (Why?)

ii. *Suppose $a, b \in \mathbb{Z}$, not both zero. Then $\dfrac{a}{\gcd(a,b)}, \dfrac{b}{\gcd(a,b)}$ are relatively prime.*

iii. *Let $a, b, c \in \mathbb{Z}$. Suppose a, b are relatively prime and a, c are relatively prime. Then a, bc are relatively prime.*

iv. *Let $a, b \in \mathbb{Z}$. Suppose a, b are relatively prime. Then a^2, b^2 are relatively prime.*

v. *Let $a, b, c \in \mathbb{Z}$. Suppose a, b are relatively prime and c is divisible by each of a, b. Then c is divisible by ab.*

9. We introduce the definition for the notion of *congruence for integers* below:

- *Let $n \in \mathbb{N}\backslash\{0, 1\}$, and $a, b \in \mathbb{Z}$. We say a is* **congruent to** *b* **modulo** *n if $a - b$ is divisible by n. We write $a \equiv b (\mathsf{mod}\ n)$.*

(a) Let $n \in \mathbb{N}\backslash\{0, 1\}$. Prove the statements:

i. *Suppose $x \in \mathbb{Z}$. Then $x \equiv x (\mathsf{mod}\ n)$.*

ii. *Let $x, y \in \mathbb{Z}$. Suppose $x \equiv y (\mathsf{mod}\ n)$. Then $y \equiv x (\mathsf{mod}\ n)$.*

iii. *Let $x, y, z \in \mathbb{Z}$. Suppose $x \equiv y (\mathsf{mod}\ n)$ and $y \equiv z (\mathsf{mod}\ n)$. Then $x \equiv z (\mathsf{mod}\ n)$.*

iv. *Let $x, y, u, v, p, q \in \mathbb{Z}$. Suppose $x \equiv u (\mathsf{mod}\ n)$ and $y \equiv v (\mathsf{mod}\ n)$. Then $px + qy \equiv pu + qv (\mathsf{mod}\ n)$.*

v.$^{\diamondsuit}$ *Let $x, y, u, v \in \mathbb{Z}$. Suppose $x \equiv u (\mathsf{mod}\ n)$ and $y \equiv v (\mathsf{mod}\ n)$. Then $xy \equiv uv (\mathsf{mod}\ n)$.*

(b)$^{\diamondsuit}$ Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}\backslash\{0, 1\}$. Suppose a, n are relatively prime. Prove the statements below:

i. *There exists some $x \in \mathbb{Z}$ such that $ax \equiv b (\mathsf{mod}\ n)$.*

ii. *For any $y, z \in \mathbb{Z}$, if $ay \equiv b (\mathsf{mod}\ n)$ and $az \equiv b (\mathsf{mod}\ n)$ then $y \equiv z (\mathsf{mod}\ n)$.*

Remark. We may combine the above results as:

($\natural$) *For any $a, b \in \mathbb{Z}$, for any $n \in \mathbb{N}\backslash\{0, 1\}$, if a, n are relatively prime then there exists some unique integer x congruent modulo n such that $ax \equiv b (\mathsf{mod}\ n)$.*

(c) Determine all solutions of each of the equations (with unknown x) below:

i. $3x \equiv 1 (\mathsf{mod}\ 5)$ ii. $6x \equiv 4 (\mathsf{mod}\ 7)$ iii. $4x \equiv 2 (\mathsf{mod}\ 9)$

(d)$^{\clubsuit}$ For each of the equations (with unknown x) below, determine whether it has any solution at all, and where it has some solution, determine all its solutions:

i. $4x \equiv 2 (\mathsf{mod}\ 6)$ ii. $4x \equiv 1 (\mathsf{mod}\ 6)$

Remark. Here the result described by the statement ($\natural$) is not applicable. (Why?)