MATH10101 JANUARY 2016 NEW STYLE: SOLUTIONS (Version 2018-01-06)

A1. Construct truth tables for the statements:

(i) Q and R
(ii) $P \not\Rightarrow Q$
(iii) (not P) or Q
(iv) not (P or (not Q))
(v) $P \Rightarrow$ (Q and R).

[5 marks]

A1. Solution (Similar to classwork and homework)

The required truth tables are:

(i)

Q	R	Q and R
T	T	T
T	F	F
F	T	F
F	F	F

(ii)

P	Q	$P \not\Rightarrow Q$
T	T	F
T	F	T
F	T	F
F	F	F

(iii)

P	Q	not P	(not P) or Q)
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

(iv)

P	Q	not Q	P or (not Q)	not (P or (not Q))
T	T	F	T	F
T	F	T	T	F
F	T	F	F	T
F	F	T	T	F

(v)

P	Q	R	Q and R	$P \Rightarrow$ (Q and R)
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	T	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

[5 marks]

A2. Prove or disprove each of the following statements:

(i) $\exists p \in \mathbb{Q}, \forall q \in \mathbb{Q}, p + q = 1/2$
(ii) $\forall q \in \mathbb{Q}, \exists p \in \mathbb{Q}, p + q = 1/2$
(iii) $\forall q \in \mathbb{Q}, \exists p \in \mathbb{Q}, p + q \neq 1/2$
(iv) $\exists p \in \mathbb{Q}, \exists q \in \mathbb{Q}, p + q < 1/2$
(v) $\forall p \in \mathbb{Q}, \forall q \in \mathbb{Q}, p + q \notin \mathbb{Z}$.

[5 marks]

A2. Solution (Similar to classwork and homework)

(i) The statement $\exists p \in \mathbb{Q}, \forall q \in \mathbb{Q}, p + q = 1/2$ is false, because $p + 0 \neq p + 1$ for any $p \in \mathbb{Q}$.
(ii) The statement $\forall q \in \mathbb{Q}, \exists p \in \mathbb{Q}, p + q = 1/2$ is true, by choosing $p = 1/2 - q$.
(iii) The statement $\forall q \in \mathbb{Q}, \exists p \in \mathbb{Q}, p + q \neq 1/2$ is true, by choosing $p = -q$.
(iv) The statement $\exists p \in \mathbb{Q}, \exists q \in \mathbb{Q}, p + q < 1/2$ is true, by choosing $p = q = 0$.
(v) The statement $\forall p \in \mathbb{Q}, \forall q \in \mathbb{Q}, p + q \notin \mathbb{Z}$ is false, because $p = q = 1/1 = 1$ implies $p + q = 2 \in \mathbb{Z}$.

[5 marks]

A3.

(i) Explain why the Diophantine equation

$$6x + 10y = 90$$

has infinitely many solutions $(x, y) \in \mathbb{Z}^2$, and describe them all.

(ii) Solve the equation in part (i) subject to the additional constraints $x > 3$ and $y > 3$.

[5 marks]

A3. Solution (Similar to classwork and homework)

(i) The gcd of 6 and 10 is 2, which is a factor of 90; so there are infinitely many solutions. We find a particular solution by applying Bezout's Lemma (by inspection):

$$2 = 6 \times 2 + 10 \times (-1)$$

and then multiplying by 45:

$$90 = 6 \times 90 + 10 \times (-45).$$

Thus $(x, y) = (90, -45)$ is a particular solution. Therefore the general solution is

$$(x, y) = \left(90 + t\frac{10}{2},\ -45 - t\frac{6}{2}\right) = (90 + 5t,\ -45 - 3t) \quad \forall t \in \mathbb{Z}.$$

(ii) Solving for t using the constraints $90 + 5t > 3$ and $-45 - 3t > 3$ yields

$$-17.4 = -87/5 < t < -48/3 = -16$$

and so there is a unique solution corresponding to $t = -17$, namely

$$(90 + 5 \times (-17), -45 - 3 \times (-17)) = (5, 6).$$

[5 marks]

A4.

(i) Find the multiplicative inverse of 13 mod 31.

(ii) Hence or otherwise, solve the congruence

$$13x \equiv 7 \bmod 31.$$

(iii) Use modular arithmetic and the method of successive squaring to calculate the least positive residue of

$$37^{514} \bmod 7.$$

[5 marks]

A4. Solution (Similar to classwork and homework)

(i) We require x such that $13x \equiv 1 \bmod 31$; that is

$$13x + 31y = 1.$$

This is possible since 13 and 31 are coprime. Using the Euclidean algorithm:

$$\begin{aligned} 31 &= 13 \times 2 + 5 \\ 13 &= 5 \times 2 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \end{aligned}$$

and working backwards

$$1 = 13 \times 12 + 31 \times (-5).$$

Thus the inverse of 13 mod 31 is 12 mod 31.

(ii) By above

$$13x \equiv 7 \bmod 31 \Rightarrow 12 \times 13x \equiv 12 \times 7 \bmod 31 \Rightarrow x \equiv 84 \bmod 31 \equiv 22 \bmod 31.$$

(iii) We have

$$\begin{aligned} 37^{514} \bmod 7 &\equiv 2^{514} \bmod 7 \\ &\equiv 2^{512}2^2 \bmod 7 \\ &\equiv 2^{512}4 \bmod 7 \\ &\equiv (2^3)^{170}2^2 4 \bmod 7 \\ &\equiv 16 \bmod 7 \\ &\equiv 2 \bmod 7. \end{aligned}$$

[5 marks]

A5.

(i) Define what is meant by a *permutation* of the finite set $X = \{1, 2, \ldots, n\}$.

(ii) Write each of the following three permutations in disjoint cycle form:

$$(3\,4\,2)(2\,5\,3), \qquad \Big((2\,4\,3)(1\,5\,6\,7)\Big)^{-1}, \qquad (1\,2)(2\,3)(3\,4).$$

(iii) Determine the order of the second permutation in part (ii).

[5 marks]

A5. Solution (Bookwork, and similar to classwork and homework)

(i) A permutation is a bijection from X to itself.

(ii) These permutations may be rewritten

$$\begin{aligned} (3\,4\,2)(2\,5\,3) &= (2\,5\,4) \\ \Big((2\,4\,3)(1\,5\,6\,7)\Big)^{-1} &= (1\,7\,6\,5)(2\,3\,4) \\ (1\,2)(2\,3)(3\,4) &= (1\,2\,3\,4) \end{aligned}$$

as products of disjoint cycles.

(iii) The order of a product of disjoint cycles is the lowest common multiple of the cycle lengths. The required order is therefore $4 \times 3 = 12$.

[5 marks]

B6.

(i) For any sets A and B, define the sets $A \cap B$ and $A \cup B$. For any set C, prove that

$$(A \cap B) \cup C \supseteq (A \cap C) \cup (B \cap C),$$

and explain how this statement simplifies when $C = \emptyset$. Under what circumstances does your simplification give equality?

[5 marks]

(ii) Given disjoint finite sets D and E, state the *Addition Principle* for the cardinality of $D \cup E$. Explain the modification required when $D \cap E \neq \emptyset$. By substituting $D = A \cup B$ and $E = C$ into your formula, prove that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

for any finite sets A, B and C. [*You may use the fact that* $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ *without proof*].

[5 marks]

B6. Solution (Homework and bookwork)

(i) For any sets A and B,

$A \cap B := \{x : x \in A \text{ and } x \in B\}$ and $A \cup B := \{x : x \in A \text{ or } x \in B\}$.

For any set C, let $x \in (A \cap C) \cup (B \cap C)$. Then $x \in (A \cap C)$ or $x \in (B \cap C)$, so $x \in C$ in either case. Hence $x \in (A \cap B) \cup C$, so $(A \cap C) \cup (B \cap C) \subseteq (A \cap B) \cup C$, as required.

When $C = \varnothing$, we have that $A \cap C = B \cap C = \varnothing$, and obtain $\varnothing \subseteq A \cap B$. This is an equation iff A and B are disjoint.

[5 marks]

(ii) The Addition Principle for disjoint finite sets states that their cardinalities satisfy $|D \cup E| = |D| + |E|$. If they are not disjoint, then

(1) $$|D \cup E| = |D| + |E| - |D \cap E|.$$

Now substitute $D = A \cup B$ and $E = C$, to get

$$|A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$$

Applying (1) and the fact that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ then gives

$$|A \cup B \cup C| = |A| + |B| - |A \cap B| + |C| - (|A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|).$$

So $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$, as required.

[5 marks]

B7.

(i) Explain what is meant by an *inverse* of a function $g\colon X \to Y$, and prove that if g has an inverse, then it is a bijection. Is the converse true or false?

[5 marks]

(ii) Let $h\colon \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = \cos x$, for all $x \in \mathbb{R}$, and show that h is neither an injection nor a surjection. Find closed intervals I, $J \subset \mathbb{R}$ for which the restriction $h|_I\colon I \to J$ is a bijection. In this case, describe the inverse function.

[5 marks]

B7. Solution (Bookwork and classwork)

(i) An *inverse* of g is a function $f\colon Y \to X$ for which $f \cdot g = 1_X$ and $g \cdot f = 1_Y$. To prove that g is a bijection if it has an inverse, let the inverse be $f\colon Y \to X$. Then g is an injection, because $g(w) = g(x) \Rightarrow f(g(w)) = f(g(x)) \Rightarrow 1_X(w) = 1_X(x) \Rightarrow w = x$ for any $w, x \in X$; and g is a surjection because $g(f(y)) = y$ for any $y \in Y$.

The converse is always true; if g is a bijection, then it has an inverse.

[5 marks]

(ii) Given $h\colon \mathbb{R} \to \mathbb{R}$ by $y = h(x) = \cos x$ for any $x \in \mathbb{R}$, observe that $\cos \pi/2 = \cos 3\pi/2 = 0$, so cos is not injective; and that $|\cos x| \leq 1$ for every $x \in \mathbb{R}$, so cos is not surjective because no $x \in \mathbb{R}$ can satisfy $\cos x = 2$.

But cos is monotonic decreasing on the interval $I := [0, \pi]$, because $\cos 0 = 1$, $\cos \pi = -1$ and has derivative satisfying $-\sin x \leq 0$ for all $0 \leq x \leq \pi$; so cos is injective on I. This also shows that cos is surjective if its codomain is restricted to the interval $J := [-1, 1]$. Hence the restriction $\cos|_I\colon I \to J$ is bijective. The inverse function is known as $\cos^{-1}$ or $\arccos\colon J \to I$.

[5 marks]

B8.

(i) For non-negative integers k, n such that $k \leq n$, define

$$\binom{n}{k}$$

in terms of subsets of a finite set of size n, and give an explicit formula for it in terms of factorials. State the *Binomial Theorem* for expanding $(a+b)^n$ for any positive integer n and real numbers a and b; deduce that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

[5 marks]

(ii) Compute

$$\sum_{k=0}^{5} \frac{2^{3k}(-2)^{7-k}}{k!\,(5-k)!}.$$

[5 marks]

B8. Solution (Bookwork and similar to homework)

(i) By definition, $\binom{n}{k}$ is the total number of subsets of size k of any set of size n. Such a subset can be chosen in precisely

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

ways. The Binomial Theorem states that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

for any positive integer n and any real numbers a and b. Choosing $a = 1$ and $b = -1$ gives

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

as required.

[5 marks]

(ii)

$$\sum_{k=0}^{5} \frac{2^{3k}(-2)^{7-k}}{k!(5-k)!} = \frac{1}{5!} \sum_{k=0}^{5} \frac{5!}{k!(5-k)!} 8^k (-2)^{5-k} (-2)^2 = \frac{4}{5!}(8-2)^5 = \frac{6^5}{30}.$$

[5 marks]

B9.

(i) Explain what is meant by a *relation* $\sim$ on a set X, and describe the properties required for $\sim$ to be *reflexive*, *symmetric*, and *transitive*. Determine whether

$$m \sim n \;\Leftrightarrow\; m|n$$

defines an equivalence relation on $\mathbb{Z}$. [5 marks]

(ii) Given an equivalence relation $\sim$ on X, define the *equivalence class* $[x]$ for any $x \in X$, and prove that either $[x] = [y]$ or $[x] \cap [y] = \emptyset$ for any $y \in X$.
[5 marks]

B9. Solution (Bookwork)

(i) A relation is a subset of $X \times X$. A relation $\sim$ is reflexive if $x \sim x$ for all $x \in X$, is symmetric if $x \sim y$ implies $y \sim x$ for all $x, y \in X$, and is transitive if $x \sim y$ and $y \sim z$ imply $x \sim z$ for all $x, y, z \in X$. The relation given by

$$m \sim n \;\Leftrightarrow\; m|n$$

on $\mathbb{Z}$ is not symmetric, because $1 \sim 2$ but $2 \not\sim 1$. So it cannot be an equivalence relation, otherwise all three properties would hold.

[5 marks]

(ii) If $x \in X$, then $[x]$ is the set $\{y \in X : x \sim y\}$.

No $[x]$ can be empty, by reflexivity; so to prove that either $[x] = [y]$ or $[x] \cap [y] = \emptyset$ for any x, $y \in X$, it is enough to show (by taking contrapositives) that $[x] \cap [y] \neq \emptyset$ implies $[x] = [y]$. Let $w \in [x] \cap [y]$, which implies that $x \sim w$ and $y \sim w$. Hence $w \sim y$ by symmetry and $x \sim w \sim y$; so $x \sim y$ by transitivity. Thus $z \in [y]$ implies $x \sim y \sim z$, so $x \sim z$ and $z \in [x]$; similarly, $z \in [x]$ implies $z \in [y]$. Thus $[x] = [y]$, as required.

[5 marks]

B10.

(i) Explain what it means for a positive integer $p \in \mathbb{Z}^+$ to be *prime*, and prove that there are infinitely many primes in $\mathbb{Z}^+$. [*You may use the fact that every integer greater than* 1 *factorises into a product of primes in a unique way*]

[5 marks]

(ii) Let [0], [1], [2], [3], [4], [5] be the six congruence classes of the integers modulo 6; explain why there are only two primes in the set

$$[0] \cup [2] \cup [3] \cup [4] \subset \mathbb{Z},$$

and show that $x,\ y \in [1]$ implies $xy \in [1]$. By considering integers of the form $6P - 1$, deduce that [5] contains infinitely many primes.

[5 marks]

B10. Solution (Bookwork and similar to homework)

(i) A positive integer p is prime if $p > 1$ and the only positive divisors of p are p and 1. Suppose there are only finitely many primes $p_1,\ p_2,\ \ldots,\ p_k$. Let

$$N = p_1 \times p_2 \times \cdots \times p_k + 1.$$

We know that every integer greater than one factorises into a product of primes, so the same must be true of N. However, none of the primes listed above can divide N, since each leaves remainder 1. This is a contradiction, so there must be infinitely many primes.

[5 marks]

(ii) The integers contained in [0] are all divisible by 6 and so cannot be prime. The numbers contained in [2] are all divisible by 2 and so cannot be prime, apart from 2 itself. The numbers contained in [3] are all divisible by 3 and so cannot be prime, apart from 3 itself. The numbers contained in [4] are all divisible by 4 and so cannot be prime. This means that the only primes contained in the union are 2 and 3. If $x,\ y \in [1]$, then $x \equiv 1$ and $y \equiv 1 \bmod 6$, so by Modular Arithmetic $xy \equiv 1 \times 1 = 1 \bmod 6$ meaning that $xy \in [1]$.

Now suppose that $p_1,\ \ldots,\ p_k$ is a finite list of all the primes in [5], let $P = p_1 p_2 \ldots p_k$ and consider the integer

$$N = 6P - 1.$$

Note that $k \geq 1$ (since the prime 5 is in [5]) so that $N > 1$. Furthermore, N is not divisible by 2, 3, $p_1,\ \ldots p_k$ (because these primes divide $6P$ and do not divide -1) and so the unique prime factorisation of N must include only primes in [1]. However, a product of primes in [1] must also lie in [1], as shown above. Since $N \in [5]$, this is again a contradiction.

[5 marks]