SECTION A

Answer **ALL FIVE** questions

Feedback: *Below are the model solutions and the examiners' feedback to the MATH10101 January 2018 exam. The paper was rather challenging, especially towards the end, and the students were required to do all the questions. It was pleasing to see so many strong scripts. However, a small minority of students did not appropriately engage with the material taught in the course and finished way below the pass mark.*

A1. Construct truth tables for the statements:

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

A1. Solution The required truth tables are:

(i)

P	Q	$P \Leftarrow Q$
T	T	T
T	F	T
F	T	F
F	F	T

(ii)

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

(iii)

P	Q	not P	not Q	(not P) and (not Q)
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

(iv)

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

(v)

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

Feedback: *A1 was answered well, with mistakes in the first parts making up most of the lost marks. In the longer truth table students seemed to be more careful and this was almost always answered correctly.*

[5 marks]

A2. Prove or disprove each of the following statements:

(i) $\forall m \in \mathbb{Z}$, $\forall n \in \mathbb{Z}^+$, $mn \geq m$
(ii) $\exists m \in \mathbb{Z}^+$, $\exists n \in \mathbb{Z}^+$, $mn \geq m$
(iii) $\forall m \in \mathbb{Z}$, $\exists n \in \mathbb{Z}$, $m = 2n$
(iv) $\exists n \in \mathbb{Z}$, $\forall m \in \mathbb{Z}$, $m > 2n$
(v) $\exists n \in \mathbb{Z}^+$, $\forall m \in \mathbb{Z}^+$, $mn > 2m$.

A2. Solution

(i) The statement $\forall m \in \mathbb{Z}, \forall n \in \mathbb{Z}^+, mn \geq m$ is false, because $m = -1$ and $n = 2$ is a counterexample
(ii) The statement $\exists m \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+, mn \geq m$ is true, for example by choosing $m = n = 1$
(iii) The statement $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}, m = 2n$ is false, because $m = 1$ is a counterexample
(iv) The statement $\exists n \in \mathbb{Z}, \forall m \in \mathbb{Z}, m > 2n$ is false, because any $m \leq 2n$ provides a counterexample
(v) The statement $\exists n \in \mathbb{Z}^+, \forall m \in \mathbb{Z}^+, mn > 2m$ is true, for example by choosing $n = 3$.

Feedback: *This question aimed to test how well the students engaged with the basic logic which lies at the heart of the course. Although many students answered this question very well, others struggled to understand when an example/counterexample was enough and when a proof was needed. (i)–(iii) were answered better then the other two parts whereas most mistakes were made in (iv).*

[5 marks]

A3.

(i) State without proof the *factorial formula* for the binomial coefficient $\binom{n}{r}$.

Answer to (i)**:** $\binom{n}{r} = \dfrac{n!}{r!\,(n-r)!}$.

Feedback: *Done well.*

(ii) State without proof the *Binomial Theorem*.

Answer to (ii)**:** Let $a, b \in \mathbb{R}$. For all $n \geq 0$ we have

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

with the convention that $x^0 = 1$ for all $x \in \mathbb{R}$.

Feedback: *Done well — although some students missed the summation sign, ending up with an equation which made no sense at all (what is r?).*

(iii) Let $n \in \mathbb{Z}^+$. Show that $2^n n = \sum_{r=0}^{n} 2r\binom{n}{r}$ and verify this result for $n = 4$ by direct calculation.

Answer to (iii)**:** there is a number of ways to derive this identity. Each of the following proofs is correct.

Proof 1. It was shown in the course that $r\binom{n}{r} = n\binom{n-1}{r-1}$ if $1 \leq r \leq n$. The right-hand side therefore rewrites as $0\binom{n}{0} + \sum_{r=1}^{n} 2n\binom{n-1}{r-1} = 0 + 2n \times (1+1)^{n-1} = 2^n n$.

Feedback: *the step marked by arrow is explained on the next page.*

Proof 2. Differentiate both sides of the binomial formula $(1+x)^n = \sum_{r=0}^{n} \binom{n}{r} x^r$ with respect to x, obtaining $n(1+x)^{n-1} = \sum_{r=1}^{n} r\binom{n}{r} x^{r-1}$. Substituting $x = 1$ leads to $n \times 2^{n-1} = \sum_{r=1}^{n} r\binom{n}{r}$ which is equivalent to the required result. □

Proof 3. Using the fact (shown in the course) that $\binom{n}{r} = \binom{n}{n-r}$, rewrite the right-hand side as $\sum_{r=0}^{n} r\binom{n}{r} + \sum_{r=0}^{n} r\binom{n}{n-r}$, or, after changing the summation variable to $n-r$ in the second sum, $\sum_{r=0}^{n} r\binom{n}{r} + \sum_{r=0}^{n} (n-r)\binom{n}{r} = \sum_{r=0}^{n} n\binom{n}{r} = n \times 2^n$. □

Verification for $n = 4$: one has $64 = 0 + 2\binom{4}{1} + 4\binom{4}{2} + 6\binom{4}{3} + 8\binom{4}{4} = 0 + 2 \times 4 + 4 \times 6 + 6 \times 4 + 8 \times 1 = 0 + 8 + 24 + 24 + 8$, true.

Feedback: *The question posed significant difficulty to many. Proof 1 was the most popular solution — among those who managed to do the question; some offered an induction argument based on the same idea as Proof 1 but with mixed results. Some were hindered by gross arithmetic mistakes such as* $2 \times 0 = 2$ *!*

Explanation of the step $\sum_{r=1}^{n} 2n\binom{n-1}{r-1} = 2n \times (1+1)^{n-1}$ (*added 2019-12-21. This explanation was not necessary for the mark but attempts to show the thought processes by which this step could be made.*).

By taking out the common factor of $2n$, the left-hand side is equal to

(†) $$2n \sum_{r=1}^{n} \binom{n-1}{r-1}.$$

To simplify (†), we would like to use the Binomial Theorem from part (ii). Note that the sum in Binomial Theorem (as stated) involves binomial coefficients $\binom{n}{r}$ whereas (†) involves $\binom{n-1}{r-1}$. Hence we need **the Binomial Theorem for $n-1$** (replace n by $n-1$ in the Theorem): *Let* $a, b \in \mathbb{R}$. *For all* $n \geq 1$ *we have*

$$(a+b)^{n-1} = \sum_{r=0}^{n-1} \binom{n-1}{r} a^{n-1-r} b^r$$

with the convention that $x^0 = 1$ *for all* $x \in \mathbb{R}$.

We now observe that the sum in the Theorem must go from 0 to $n-1$ whereas in (†), r runs from 1 to n. Let us change the summation variable in (†) to $s = r-1$. Then (†) becomes

$$2n \sum_{s=0}^{n-1} \binom{n-1}{s}$$

which can be written as

$$2n \sum_{s=0}^{n-1} \binom{n-1}{s} 1^{n-1-s} 1^s.$$

By the Binomial Theorem for $n-1$, this is exactly the expansion of $2n \times (1+1)^{n-1}$, as claimed.

[5 marks]

A4.

(i) Let a, b, c be integers. State the criterion for the equation $ax + by = c$ to have at least one solution $(x, y) \in \mathbb{Z}^2$.

Answer to (i)**:** this equation has solutions, if and only if $\boldsymbol{\gcd(a, b) \mid c}$.

Feedback: *Some students couldn't answer part (i) but then used the correct criterion in later parts of the question, indicating they had learnt the practical method but maybe not the theoretical details.*

(ii) Describe all the solutions $(x, y) \in \mathbb{Z}^2$ of the equation

$$19x + 8y = 3.$$

Answer to (ii)**:** $(1, -2)$ is a particular solution (by inspection), $\gcd(19, 8) = 1$ so the general solution is

$$\boldsymbol{(x, y) = (1 - 8t,\ -2 + 19t), \quad t \in \mathbb{Z}.}$$

Alternatively, a particular solution can be found via Euclid's algorithm: $19\times3+8\times(-7) = 1$, multiply through by 3 to see that $(9, -21)$ is a solution, hence $\boldsymbol{(9 - 8t,\ -21 + 19t)}$, $\boldsymbol{t \in \mathbb{Z}}$ is the general solution (presented in a slightly different form).

Feedback: *Done well. Many opted to go via Euclid's algorithm, although this should have taken longer than finding a particular solution by inspection.*

(iii) Now consider the equation $19x+by = 3$. List all the integer values of b such that this equation has *no integer solutions* and $0 \leq b \leq 100$. You do not have to justify your answer.

Answer to (iii)**:** $\boldsymbol{b = 0}$, **19**, **38**, **57**, **76** or **95**.

Explanation (*not required*): If b is one of these multiples of 19, the left-hand side of the equation is divisible by 19 hence cannot equal 3. Otherwise, $\gcd(19, b) = 1$ (since the only divisors of 19 are 1 and 19) hence by part (i) the equation has solutions.

Feedback: *Many students missed the value* $b = 0$. *Note that* 0 *is a multiple of* 19. *Some missed* 19 *as well.*

[5 marks]

A5.

(i) Find all the possible remainders that $a^6 - 3a^2 + 2$, where $a \in \mathbb{Z}$, can leave when divided by 9. Show that if a is not divisible by 3 then $a^6 - 3a^2 + 2$ is divisible by 9.

Answer to (i)**:**

$a \bmod 9$	0	1	2	3	4	5	6	7	8
$a^2 \bmod 9$	0	1	4	0	7	7	0	4	1
$3a^2 \bmod 9$	0	3	3	0	3	3	0	3	3
$a^6 = (a^2)^3 \bmod 9$	0	1	1	0	1	1	0	1	1
$(a^6 - 3a^2 + 2) \bmod 9$	2	0	0	2	0	0	2	0	0

From the table, the possible remainders of $a^6 - 3a^2 + 2$ modulo 9 are 0 and 2.

If a is not a multiple of 3, then a is congruent to 1, 2, 4, 5, 7 or 8 modulo 9, hence the above table shows that $a^6 - 3a^2 + 2 \equiv 0 \bmod 9$ as required.

(*Alternatively*, notice that $a^6 - 3a^2 + 2 = (a^2 - 1)^2(a^2 + 2)$. If $3 \nmid a$, then $a^2 \equiv 1 \bmod 3$ hence both $a^2 - 1$ and $a^2 + 2$ are multiples of 3. This shows that the product is in fact divisible by 27.)

Feedback: *A5 was answered worse in general than A1–A4, although many students managed part (i) which was fairly standard.*

(ii) Use the result of (i) to find all $n \in \mathbb{Z}^+$ such that $(n! + 1)^{6n} - 3(n! + 1)^{2n} + 2$ is divisible by 9. Explain how you arrived at the answer.

Answer to (ii)**:** $n \neq 2$.

Indeed, if $n \geq 3$, then $n!$ is a multiple of 3 so $n! + 1$ is not. If $n = 1$, then $n! + 1$ is again not a multiple of 3. In these cases, putting $a = (n! + 1)^n$ we see that a is not divisible by 3, hence by the result of (i), $(n! + 1)^{6n} - 3(n! + 1)^{2n} + 2 = a^6 - 3a^2 + 2$ is divisible by 9.

In the remaining case $n = 2$, both $(n! + 1)^{6n}$ and $(n! + 1)^{2n}$ are multiples of 9 hence $(n! + 1)^{6n} - 3(n! + 1)^{2n} + 2$ is not divisible by 9.

Feedback: *Only a small percentage of students were able to get full marks in (ii). Some students almost answered (ii) fully but missed out that a should be $(n! + 1)^n$ not just $(n! + 1)$ — this was wrong. Some students forgot to check the case $n = 2$. A large portion of students didn't seem to understand how to apply part (i).*

[5 marks]

Feedback on Questions B6, B7

I was a little disappointed by the overall response to these two questions, both of which (with minor changes of data) had appeared on past papers. It suggests that rather a lot of students don't actually read this sort of feedback! Nevertheless, a considerable number answered them well, and scored close to full marks on both. Generally speaking, B6 was done better than B7.

Question B6

The marks for this question were reasonably good, in spite of the following.

- Many students did not understand that the addition principle is a statement about *disjoint* sets, which has to be modified (no proof requested) when their intersection is non-empty.
- In spite of my rants in lectures, many students wrote equations that (1) referred to the non-existant *addition* of sets, and/or (2) mixed sets and integers together. Both of these horrors suggest a lack of focus on the most elementary aspects of set theory.
- Some students' answers consisted of strings of seemingly unconnected symbols dotted around the page. Even if the correct answer was in there somewhere, it was impossible to give many marks when no mathematical reasoning was visible.
- Bafflingly, a few answers involved probability!

Question B7

This was done less well (and less often) than B6. A significant number of students had clearly decided to ignore the subject of countability, in spite of my efforts to place it at the heart of the first twenty lectures.

- Many students appear not to know what the decimal notation $0.a_1a_2\ldots$ actually means, and that to express 3/7 in this form it is sufficient to long divide 3 by 7. A few students even divided 7 by 3, and did not seem worried by getting an answer that began with $2.3\ldots$.
- About half of those who answered part (ii) appeared to think that infinite and uncountable are the same. I was lenient on the point that X must not be finite, happy to see the statement that its elements cannot be listed, and generous in marking any attempt to give Cantor's diagonal argument for $(0,1)$ (well done those who nailed it!) I even gave marks for the cheeky answer that $(0,1)$ is equipotent with $\mathbb{R}$ – in spite of proving that $\mathbb{R}$ is uncountable in lectures by doing $(0,1)$ first!

Nige

SECTION B

Answer **ALL FIVE** questions

B6.

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

$$|C \cup D \cup E| \;=\; |C| + |D| + |E| - |C \cap D| - |C \cap E| - |D \cap E| + |C \cap D \cap E|$$

for any finite sets C, D and E. [*You may assume the distributive law for* $\cup$ *and* $\cap$ *without proof*]. [5 marks]

(ii) Each of a collection of 145 pullovers is either long or short, green or black, and woollen or cotton. There are 75 long pullovers, 69 green pullovers, 60 woollen pullovers, 38 long green pullovers, 40 long woollen pullovers, 36 green woollen pullovers, and 23 long green woollen pullovers. Use part (i) to calculate the number of short black cotton pullovers. [5 marks]

B6. Solution

(i) For disjoint finite sets A and B, the *addition principle* states that $|A \cup B| = |A| + |B|$. If $A \cap B \neq \emptyset$, then

$$|A \cup B| = |A| + |B| - |A \cap B|, \tag{1}$$

in order to avoid counting the elements of $A \cap B$ twice.

Now write $A = C \cup D$ and $B = E$. Then

$$\begin{aligned} |C \cup D \cup E| \;=\; |(C \cup D) \cup E| \;&=\; |C \cup D| + |E| - |(C \cup D) \cap E| \\ &=\; |C| + |D| + |E| - |C \cap D| - |(C \cap E) \cup (D \cap E)| \end{aligned} \tag{2}$$

by (1) and the distributivity law. But $|(C \cap E) \cup (D \cap E)| = |C \cap E| + |D \cap E| - |C \cap D \cap E|$, by (1) again. Substituting into (2) then gives

$$|C \cup D \cup E| = |C| + |D| + |E| - |C \cap D| - |C \cap E| - |D \cap E| + |C \cap D \cap E|,$$

as required.

[5 marks]

(ii) Let J be the set of all pullovers, and let A, B, and C be the subsets of long, green, and woollen pullovers respectively. Then the data give cardinalities $|A| = 75$, $|B| = 69$, $|C| = 60$, $|A \cap B| = 38$, $|A \cap C| = 40$, $|B \cap C| = 36$, and $|A \cap B \cap C| = 23$. Substituting in (i) gives

$$|A \cup B \cup C| \;=\; 75 + 69 + 60 - 38 - 40 - 36 + 23 \;=\; 113.$$

There are therefore 113 pullovers that are long or green or woollen, and $J = (A \cup B \cup C) \cup T$, where T is the set of pullovers that are short and black and cotton. By the addition principle, $145 = |J| = 113 + |T|$, and $|T| = 32$, as required.

[5 marks]

B7.

(i) Express the *decimal* $0 \cdot a_1 a_2 \dots a_n$ as a rational number, where $0 \leq a_k \leq 9$ for each integer $a_1, \dots, a_n$. Explain how *infinite decimals* may be used to represent real numbers r in the interval $(0,1) \subset \mathbb{R}$, and compute the infinite decimal representing the rational number $3/7$.

[5 marks]

(ii) Define the term *uncountable set*, and prove that the interval $(0,1)$ is uncountable.

[5 marks]

B7. Solution

(i) The expression $0 \cdot a_1 a_2 \dots a_n$, where $a_k \in \mathbb{Z}$ satisfies $0 \leq a_k \leq 9$ for $i \geq 1$, represents the rational number

$$a_1/10 + \dots + a_k/10^k + \dots + a_n/10^n \;=\; (10^{n-1}a_1 + \dots + 10^{n-k}a_k + \dots + a_n)/10^n.$$

The expression $0 \cdot a_1 a_2 \dots a_i \dots$ represents the infinite sum $a_1/10 + \dots + a_k/10^k + \dots$, which may be described as the unique real number a satisfying

$$0 \cdot a_1 a_2 \dots a_n \leq a \leq 0 \cdot a_1 a_2 \dots a_n + 1/10^n \quad \text{for every } n \in \mathbb{Z}^+.$$

Long dividing 7 into 3 gives the recurring decimal $\frac{3}{7} = 0 \cdot \overline{428571}$.

[5 marks]

(ii) An *uncountable set* X is one that is not finite and admits no bijection $f\colon \mathbb{Z}^+ \to X$.

To prove that $(0,1)$ is uncountable, observe that this set is infinite. Suppose that there does exist a bijection $f\colon \mathbb{Z}^+ \to (0,1)$, and represent each $f(m)$ as a unique infinite decimal $0 \cdot a_{m,1} a_{m,2} \dots a_{m,k} \dots$, (with no $\overline{9}$s). Construct $b = 0 \cdot b_1 b_2 \dots b_k \dots$ by choosing $b_k = 1$ if $a_{k,k} = 0$, and $b_k = 0$ otherwise. So b differs from $f(m)$ in the mth digit, for every $m \geq 1$. Therefore b is not of the form $f(m)$ for any m, and f cannot be surjective; this is a contradiction, and confirms that $(0,1)$ admits no such bijection f.

[5 marks]

B8. Let a and b be integers, at least one of which is not 0.

(i) Give the definition of the *greatest common divisor*, $\gcd(a, b)$, of a and b. Prove the lemma which says that if $a = bq + r$ with $q, r \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, r)$. Give an example which shows that in this situation $\gcd(a, b)$ may not be equal to $\gcd(a, r)$.

Answer to (i) **:** $\gcd(a, b)$ is an integer d such that
(1) d is a common divisor of a and b, that is, $d \mid a$ and $d \mid b$;
(2) if c is a common divisor of a and b then $c \leq d$.

Suppose that $a = bq + r$ with $q, r \in \mathbb{Z}$. Since the gcd is defined as the greatest among the common divisors, it is enough to prove that c is a common divisor of a and b if and only if c is a common divisor of b and r. First, assume that $c \mid a$ and $c \mid b$. Since $r = 1a + (-q)b$ is an integral linear combination of a and b, by a fact from the course $c \mid r$. Hence c is a common divisor of b and r. Next, assume that $c \mid b$ and $c \mid r$. Since $a = qb + 1r$ is an integral linear combination of b and r, in the same way we conclude that c is a common divisor of a and b, QED.

Example: $a = 100$, $b = 1$, $100 = 1 \times 100 + 0$, put $q = 100$ and $r = 0$; one has $\gcd(a, b) = 1$ but $\gcd(a, r) = 100$.

> **Feedback:** *The most common mistake in the proof that* $\gcd(a, b) = \gcd(b, r)$ *was to give an argument which proved only one implication out of two in the* if and only if *above. There were many correct examples where* $\gcd(a, b) \neq \gcd(a, r)$ *but some students gave examples where* $a \neq bq + r$ *or where* $\gcd(a, b) = \gcd(a, r)$ *— such incorrect examples were not worth any marks.*

[5 marks]

(ii) *In the second part of the question, you are allowed to use the fact that there exist integers* m, n *such that* $\gcd(a, b) = am + bn$, *and you do not have to prove it.*

State what is meant by saying that a, b are coprime. Prove that a, b are coprime, if and only if $ap + bq = 1$ for some integers p, q. Now assume that a is odd and $b = a + 2$; show that $a + b$ and ab are coprime.

Answer to (ii) **:** "coprime" means that $\gcd(a, b) = 1$.

If a, b are coprime, then by the fact given above (Bezout's Lemma) there are $p, q \in \mathbb{Z}$ such that $1 = \gcd(a, b) = ap + bq$. The reverse implication: assume $1 = ap + bq$. Since $d = \gcd(a, b)$ is a common divisor of a and b, it is also a divisor of $1 = ap + bq$; the only non-negative divisor of 1 is 1, hence $d = 1$ as required.

Write the odd a as $2k - 1$, then $b = 2k + 1$ where $k \in \mathbb{Z}$. The integers $a + b = 4k$ and $ab = 4k^2 - 1$ satisfy $(a + b)k + ab(-1) = 1$. Hence they are coprime by the previous result.

> **Feedback:** *Again, it was quite common to see a proof of only one implication out of two in* if and only if. *When proving coprimality of* $a + b$ *and* ab, *a considerable number of students noticed that* $a + b$ *was even and* ab *was odd and then wrote a shocking statement that an even number is always coprime to an odd number. This statement is of course false (e.g.,* 6 *is not coprime to* 9*) hence such attempts were not worth any marks.*

[5 marks]

B9.

(i) Give the definition of a *prime number*. Assuming that p is a prime number, show that for any integer a, if p divides a^2 then p^2 divides a^2. (*You may use any facts from the course provided that you carefully state them.*) Now assume that an integer $n \geq 2$ is such that for any integer a, if n divides a^2 then n^2 divides a^2. Is n necessarily prime? Justify your answer.

Answer to (i) **:** $p \in \mathbb{Z}$ is a prime number if $p > 1$ and the only positive divisors of p are p and 1.

We use the lemma known as *Euclid's property of a prime*: if p is a prime, $a, b \in \mathbb{Z}$, $p \,|\, ab$, then $p \,|\, a$ or $p \,|\, b$. Apply this lemma to the case $a = b$ to conclude that if $p \,|\, a^2$ then $p \,|\, a$. Hence $a = mp$ with $m \in \mathbb{Z}$, so that $a^2 = (m^2)p^2$ is divisible by p^2.

No, n does not have to be a prime number. Indeed, let $n = 6$ which is not prime, and assume than $n \,|\, a^2$ where a is an integer. Then $2 \,|\, a^2$ and $3 \,|\, a^2$, so (similarly to the above) $2 \,|\, a$ and $3 \,|\, a$; furthermore, 2 and 3 are distinct primes so a is divisible by $2 \times 3 = n$ hence n^2 divides a^2.

Remark. Any n which is a product of distinct primes (such integers are termed *square-free*) will afford a counterexample in the same way as $n = 6$.

Feedback: *Sadly, many students made a mistake in the definition of a prime number by forgetting to state that $p > 1$. It is important to remember that, say, 1 is not a prime number (although it is only divisible by "1 and itself"). Many students tried not to use Euclid's property of a prime; some proved "$p^2 \,|\, a^2 \implies p \,|\, a^2$" which is true but trivial and was not worth marks; some used an argument based on unique prime factorisation of a, but full marks were only given if it was recognised that prime factorisation exists only for $a \geq 2$ and that other integers a had to be dealt with.*

[5 marks]

(ii) Show that there exist integers $a, b, c, d, e > 1$ such that $ab = cde$, $ac = bd^{10101}$. Do such integers exist if it is further required that e is a prime number? Justify your answer.

Answer to (ii)**:** An example to show that such integers exist is $a = 2^{10101}$, $b = c = d = 2$, $e = 2^{10100}$.

The integer e cannot be prime. Indeed, let a, b, c, d, e satisfy all the given conditions. Multiplying together the equations $ab = cde$ and $ac = bd^{10101}$, we obtain $a^2bc = bcd^{10102}e$. Since b, c are positive, we can divide by bc to obtain an equivalent equation $a^2 = f^2e$ where $f = d^{5051}$. Considering prime factorisation of both sides (which are integers greater than one), we conclude that, since a^2 is a product of an even number of primes and so is f^2, e must also be a product of an even number of primes hence not itself a prime.

One may also observe that the assumption that e is a prime leads to the rational number a/f being the square root of a prime. But the square root of a prime is irrational; particular cases of this statement arose in the course.

Feedback: *A number of valid examples of a, b, c, d, e were given, but the question about e being prime was fully solved by just a few students.*

[5 marks]

B10.

(i) Define what is meant by a *permutation* of the set $\mathbb{N}_n = \{1, 2, \ldots, n\}$. What is meant by saying that permutations σ, τ of $\mathbb{N}_n$ are *disjoint*? Prove the lemma which says that if σ and τ are disjoint, then $\sigma \circ \tau = \tau \circ \sigma$.

Answer to (i)**:** A *permutation* of any set A is a bijective function $\sigma\colon A \to A$.

For a permutation σ of A, define the set $Move(\sigma)$ as $\{a \in A \mid \sigma(a) \neq a\}$. Permutations σ and τ of A are said to be *disjoint* if $Move(\sigma) \cap Move(\tau) = \varnothing$.

Assume that permutations σ and τ of A are disjoint. We need to show that $\sigma(\tau(a)) = \tau(\sigma(a))$ where $a \in A$ is arbitrary. Since a cannot be both in $Move(\sigma)$ and in $Move(\tau)$, one has $\sigma(a) = a$ or $\tau(a) = a$; without loss of generality, assume $\sigma(a) = a$.

We claim that $\tau(a)$ is also fixed by σ. This is true if $\tau(a) = a$, since a is fixed by σ. Otherwise, $\tau(a) \neq a$; the permutation τ is a bijection hence an injection, so, applying τ to both sides, we obtain $\tau(\tau(a)) \neq \tau(a)$. This shows that $\tau(a) \in Move(\tau)$, so $\tau(a) \notin Move(\sigma)$, as claimed.

Now, using the assumption $a = \sigma(a)$, we conclude that $\sigma(\tau(a)) = \tau(a) = \tau(\sigma(a))$, QED. (*All of the above applies to* $A = \mathbb{N}_n$.)

> **Feedback:** *The only part which caused difficulty was the proof that disjoint* σ *and* τ *commute; in particular, many students failed to explain why* $\tau(a) \neq a$ *implies that* $\tau(a)$ *is not fixed by* τ*.*

[5 marks]

(ii) Assume that π, ρ are permutations of $\mathbb{N}_{20}$ such that π has order 21 and $\pi \circ \rho$ has order 24.

(a) Prove that π and ρ are not disjoint.

(b) Prove that π and $\pi \circ \rho$ are not disjoint.

(c) Write down an example of π and ρ such that the orders are as required above, or give a convincing explanation of how such an example can be constructed.

[*Any facts from the course can be used without particular comment.*]

Answer to (ii)**:** (a) Assume for contradiction that π and ρ are disjoint. Then by a fact proved in the course, the order of $\pi \circ \rho$ is the least common multiple (LCM) of the orders of π and ρ. But 24 cannot be the LCM of 21 (which is the order of π) and something else, because $21 \nmid 24$. Contradiction.

(b) Factorise π into disjoint cycles and observe that 21 must be the LCM of the lengths of these cycles. Hence π contains at least one cycle of length 7 and at least one cycle of length 3, so that $|Move(\pi)| \geq 7 + 3 = 10$.

Similarly, $\pi \circ \rho$ contains at least a cycle of length 8 and a cycle whose length is a multiple of 3 (which is at least 3). We conclude that $|Move(\pi \circ \rho)| \geq 8 + 3 = 11$.

But then the subsets $Move(\pi)$ and $Move(\pi \circ \rho)$ of $\mathbb{N}_{20}$ cannot be disjoint, since the sum of their cardinalities is greater than 20. Hence π and $\pi \circ \rho$ are not disjoint.

(c) For example, $\pi = (1, 2, 3, 4, 5, 6, 7) \circ (8, 9, 10)$ and $\pi \circ \rho = (1, 2, 3, 4, 5, 6, 7, 8) \circ (9, 10, 11)$, whereas ρ can be calculated as $\pi^{-1} \circ (\pi \circ \rho)$.

> **Feedback:** *The counting argument in (b) was the most difficult part of the solution and was often incomplete, e.g., it was claimed that* π *must contain exactly one cycle of length* 7 *— whereas it may well contain two such disjoint cycles.*

[5 marks]

END OF EXAMINATION PAPER