Below are the model solutions and the examiners feedback to the MATH10101 January 2019 exam. The paper succeeded in thoroughly testing the students' knowledge of a wide selection of topics covered in the course. To achieve a strong result, students also had to show that they can carefully construct a rigorous mathematical argument. There was a considerable number of first class results, indicating that the student had attained practically all of the ILOs tested by the paper at a high level. However, the paper was challenging, and there was a sizeable set of scripts falling short of the pass mark, which meant significant gaps in attainment already in Section A.

The feedback below indicates which questions were done well, and which ones turned out to be difficult.

The exam paper tests the following Intended Learning Outcomes (ILO) of the course:

ILO1 Analyse the meaning of mathematical statements involving quantifiers and logical connectives, and construct the negation of a given statement.

ILO2 Construct truth tables of simple mathematical statements and use these to determine whether two given statements are equivalent.

ILO3 Construct elementary proofs of mathematical statements using a range of fundamental proof techniques (direct argumentation, induction, contradiction, use of contrapositive).

ILO4 Use basic set theoretic language and constructions to prove results about finite, denumerable and uncountable sets.

ILO5 Use elementary counting arguments, such as the pigeonhole principle, the inclusion-exclusion formula and the binomial theorem to compute cardinalities of finite sets and simplify expressions involving binomial coefficients.

ILO6 Recall formal definitions and apply these to give examples and non-examples of functions, bijections, equivalence relations, binary operations and groups.

ILO7 Recall and justify basic number-theoretic methods, including the Euclidean algorithm, and use them to solve simple arithmetic problems such as linear Diophantine equations.

ILO8 Use modular arithmetic to solve linear and simple non-linear congruences.

ILO9 Recall the fundamental properties of prime numbers, prove their infinitude and solve elementary problems on primes and prime factorisation.

ILO10 State and prove Fermat's Little Theorem and Euler's theorem and apply them to solving simple questions involving primality testing and Euler's phi-function.

ILO11 Recognise the two-line notation and the cycle notation for permutations and use them to compose, invert and find the order of given permutations.

SECTION A

Answer **ALL FIVE** questions

A1.

(i) Write down the negation of the statement

$$\forall x \in \mathbb{R},\, \exists y \in \mathbb{R},\, x > 3y.$$

State whether the statement or its negation is true. Explain your answer.

(ii) Write down the contrapositive of the statement

'For any $n \in \mathbb{Z}$, if 5 does not divide n^2, then 5 does not divide n.'

Prove the statement is true.

[5 marks]

A1. Solution ILO1 at low and medium levels.

(i) The negation is $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x \leq 3y$. The original statement is true because given any $x \in \mathbb{R}$, let $y = (x-1)/3 \in \mathbb{R}$. Then $x > 3y$.

[2 marks]

(ii) The contrapositive is 'For any $n \in \mathbb{Z}$, if 5 divides n, then 5 divides n^2.' To prove the contrapositive assume $5 \,|\, n$, i.e. $n = 5k$ for some $k \in \mathbb{Z}$. Then $n^2 = 25k^2 = 5(5k^2)$ and so 5 divides n^2. Since the contrapositive is logically equivalent to the original statement, the statement is true.

[3 marks]

A1. Feedback Most mistakes were made in part (i). Almost everyone wrote the negation correctly, the mistakes were in proving/disproving the statements. The most common things were trying to disprove the negation by giving a counterexample with a particular value of x (which didn't work as it started with "there exists..."), or proving the original statement by picking $y = x/4$, which fails for negative values of x. Part (ii) was generally done correctly.

A2.

(i) Let A and B be subsets of a universal set U. Prove that $(A \cup B)^c = A^c \cap B^c$.

(ii) Let $A = \{1, 2, 3\}$ and let the function $f : A \times A \to \mathbb{Z}$ be defined by $f((a, b)) = a - b$. Write down $\operatorname{Im} f$, listing all the elements.

Is f injective? Explain your answer.

(iii) State the Pigeonhole Principle.

[5 marks]

A2. Solution (i) ILO2 and ILO4 at low level, (ii,iii) ILO4 and ILO6 at medium level.

(i) Using truth tables,

$x \in A$	$x \in B$	$x \in (A \cup B)^c$	$x \in A^c \cap B^c$
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

Since the final two columns are the same, we have $(A \cup B)^c = A^c \cap B^c$. Students may also prove that each set is a subset of the other. [2 marks]

(ii) $\operatorname{Im} f = \{-2, -1, 0, 1, 2\}$. [1 mark]

f is not injective because $f((1, 1)) = f((2, 2))$ [1 mark]

(iii) If A and B are finite sets with $|A| > |B|$, then any function $f : A \to B$ is not injective. [1 mark]

A2. Feedback Part (i) turned out to be a big source of mistakes. The most common were:

- treating sets as logical statements in the truth tables;
- proving only one of the inclusions between sets. This is probably a mistake the students might struggle to recognise, since most of the time it wasn't done explicitly, in the following sense: the student usually started with "take $x \in (A \cup B)^c$", and with a series of implications obtained that x belongs to the other set, then claimed equality of sets;
- using equalities between sets that they didn't prove, or working with cardinality of sets.

In quite a few cases students gave a proof by just drawing Venn diagrams, which was not considered a correct answer.

Part (ii) was generally done correctly, while in many instances the students failed to write down the pigeonhole principle in part (iii).

A3.

(i) Use the method of successive squaring to find the remainder of 2^{65} when divided by 100.

(ii) Hence or otherwise, find the last two decimal digits of 798^{65}.

(iii) You are given that $n \in \mathbb{N}$ is such that 2^n leaves remainder 2 when divided by 100. Prove by contradiction that $n = 1$.

[5 marks]

A3. Solution ILO7, ILO8 at a medium level

(i) Calculation: $2^2 \equiv 4 \mod 100$, hence

$2^4 \equiv 4^2 \equiv 16 \mod 100$, hence

$2^8 \equiv 16^2 \equiv 56 \mod 100$, hence

$2^{16} \equiv 56^2 \equiv 36 \mod 100$, hence

$2^{32} \equiv 36^2 \equiv 96 \mod 100$, hence

$2^{64} \equiv 96^2 \equiv (-4)^2 \equiv 16 \mod 100$.

One has $2^{65} = 2 \times 2^{64} \equiv 2 \times 16 \equiv 32 \mod 100$.
Therefore, the remainder left by 2^{65} when divided by 100 is $\mathbf{32}$. [2 marks]

(ii) Observe that $798 \equiv -2 \mod 100$, hence $798^{65} \equiv (-2)^{65} \equiv -2^{65} \equiv -32 \equiv 68 \mod 100$. This shows that 798^{65} leaves remainder 68 when divided by 100. Hence the last two decimal digits of 798^{65} are $\mathbf{68}$. [1 mark]

(iii) Assume for contradiction that $n \neq 1$. Since $n \in \mathbb{N}$, this means that $n \geq 2$. It follows that 2^n is divisible by $2^2 = 4$. On the other hand, we are given that $2^n = 100k + 2$ for some $k \in \mathbb{Z}$. Note that $100k$ is divisible by 4, and 2 is not divisible by 4. Hence $100k + 2$ is not divisible by 4 and cannot equal 2^n, a contradiction. Therefore, the assumption $n \neq 1$ was false. [2 marks]

A3. Feedback (i) Mostly done well. (ii) The typical mistakes were stating that $798^{65} \equiv 32 \mod 100$ and claiming that the last two digits of 798^{65} were "-32". (iii) Mistakes included: assuming that $n = 1$ and arriving at $2^n \equiv 2 \mod 100$ — this is trivially true but does not answer the question; and trying to use the the particular powers of 2 occurring in (i) to make a conclusion for all n — this is not rigorous and at the very least is not proof by contradiction.

A4. Let $\phi\colon \mathbb{N} \to \mathbb{N}$ be Euler's phi-function. Let p, q be prime numbers such that $p \neq q$, and let $k \in \mathbb{N}$.

(i) Write down a formula for $\dfrac{\phi((pq)^k)}{(pq)^k}$.

(ii) Hence or otherwise, show that $10^{-k}\phi(10^k) = 0.4$.

(iii) Is it possible for $\phi((pq)^k)$ to be a prime number? Explain your answer.

[5 marks]

A4. Solution ILO9 at a low level, ILO10 at a medium level

(i) $\dfrac{\phi((pq)^k)}{(pq)^k} = (1-p^{-1})(1-q^{-1})$ (*or equivalent*).

Explanation (*not required*): it was shown in the course that $\phi(p^k) = p^{k-1}(p-1)$ for primes p, hence also $\phi(q^k) = q^{k-1}(q-1)$. Since p^k, q^k are coprime, $\phi((pq)^k) = \phi(p^kq^k) = p^{k-1}(p-1)q^{k-1}(q-1)$ by multiplicativity of ϕ. Divide this by p^kq^k to obtain the formula given above. [2 marks]

(ii) Substituting the primes $p = 2$, $q = 5$ in (i), we obtain

$$10^{-k}\phi(10^k) = \frac{\phi((2\times 5)^k)}{(2\times 5)^k} = (1-2^{-1})(1-5^{-1}) = 0.5 \times 0.8 = 0.4.$$ [1 mark]

(iii) Yes, $\phi((pq)^k)$ can be a prime. Take $p = 2$, $q = 3$, $k = 1$. Then $\phi((pq)^k) = \phi(6) = 2$ is a prime. This is the only possible example up to permutation of p, q. [2 marks]

A4. Feedback Although (i,ii) were done reasonably well overall, some students made the following erroneous assumptions:

(a) $(\phi(p))^k = \phi(p^k)$ when p is a prime. This is wrong since $\phi(p^k) = p^{k-1}(p-1)$.

(b) $\phi((pq)^k) = (pq-1)^k$ when p, q are primes. This is also wrong since $\gcd(p, q) = 1$ implies $\phi((pq)^k) = \phi(p^k)\phi(q^k)$.

In (ii), students who left the answer to (i) in terms of k found it difficult to eliminate k, or assumed $k = 1$ which was not given.

Not many answered (iii) correctly, providing the unique example.

A5. The permutations $\rho, \sigma, \tau \in S_8$ are given by

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}, \ \sigma = (1,2) \circ (2,3) \circ (3,4) \circ (4,5) \circ (2,3) \circ (1,2), \ \tau = \rho \circ \sigma \circ \rho^{-1}.$$

(i) By writing τ as a product of disjoint cycles, show that τ is a cycle of length 3. State the order of τ.

(ii) How many cycles of length 3 are there in S_8? Explain your answer briefly. (Your answer may contain binomial coefficients or factorials, and you do not have to calculate their numerical values.)

[5 marks]

A5. Solution ILO11 at a low level, ILO5 at a medium level

(i) To write τ as a product of disjoint cycles, we first rewrite ρ, σ and ρ^{-1} in two-line notation:

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}, \ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 5 & 1 & 6 & 7 & 8 \end{pmatrix}, \ \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

We now compute $\tau(1) = \rho(\sigma(\rho^{-1}(1))) = 1$, $\tau(2) = \rho(\sigma(\rho^{-1}(2))) = 5$, and so on. We find that the numbers $1, 3, 4, 7, 8$ are fixed by τ and that $\tau(2) = 5$, $\tau(5) = 6$ and $\tau(6) = 2$. Hence $\tau = (2, 5, 6)$, a cycle of length 3. The order of τ is 3. [3 marks]

(ii) A cycle (a, b, c) of length 3 corresponds to the subset $\{a, b, c\}$ of cardinality 3 of $\mathbb{N}_8 = \{1, 2, \ldots, 8\}$. In fact, $\{a, b, c\}$ is the set $Move((a, b, c))$. Each set $\{a, b, c\}$ of cardinality 3 thus corresponds to two distinct cycles of length 3, (a, b, c) and (a, c, b), as putting a, b and c in any order gives one of these two cycles. Therefore, the number of cycles of length 3 is twice the number of subsets of size 3 of $\mathbb{N}_8$.

Answer: $2 \times \binom{8}{3}$. Numerical answer (*not necessary*): 112. [2 marks]

A5. Feedback (i) Overall this question was answered well. Most students who were able to write σ correctly in 2-line notation were also able to simplify $\tau = \rho\sigma\rho^{-1}$ correctly and deduced that a cycle of length 3 is also of order 3.

(ii) For most students the difficulty in answering this question was the confusion between the binomial coefficient $\binom{n}{r}$ and the number of cycles in S_n. Some arrived at the answer by stating that there are $8 \times 7 \times 6$ ordered triples a, b, c but three triples: a, b, c and b, c, a as well as c, a, b give rise to the same cycle in S_8. Hence the answer was $(8 \times 7 \times 6)/3$ which is correct.

However, some lost or gained a factor of 2 due to partially incorrect reasoning, and typically got partial marks.

SECTION B

Answer **ALL FIVE** questions

B6.

(i) Let $P(n)$ be a predicate. Describe the method of simple induction used to prove that $P(n)$ is true for all $n \in \mathbb{N}$. [2 marks]

(ii) Use simple induction to prove that $2^{n-1} \leq n!$ for all $n \in \mathbb{N}$. [4 marks]

(iii) Let $f : \mathbb{R} \to \mathbb{R}\backslash\{0\}$ and $g : \mathbb{R}\backslash\{0\} \to \mathbb{R}^+$ be defined by

$$f(x) = e^x, \text{ for all } x \in \mathbb{R}, \qquad g(x) = \frac{1}{x^2} \text{ for all } x \in \mathbb{R}\backslash\{0\}.$$

Write down $g \circ f$, stating the domain and codomain. Is $g \circ f$ surjective? Explain your answer. [4 marks]

B6. Solution (i) ILO3 at low level, (ii) ILO3 at high level, (iii) ILO6 at medium level.

(i) First prove that $P(1)$ is true (base case). Next let $k \in \mathbb{N}$ and prove $P(k) \Rightarrow P(k+1)$ (inductive step). By simple induction, $P(n)$ is true for all $n \in \mathbb{N}$. [2 marks]

(ii) Let $P(n)$ be the statement $2^{n-1} \leq n!$ for all $n \in \mathbb{N}$. Since $2^0 = 1 \leq 1!$, $P(1)$ is true. Let $k \in \mathbb{N}$ and assume $P(k)$ is true, ie. $2^{k-1} \leq k!$. Then

$$2^k = 2.2^{k-1} \leq 2.k! \leq (k+1)k! = (k+1)!$$

because $2 \leq (k+1)$. Therefore $P(k+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$. [4 marks]

(iii) $g \circ f : \mathbb{R} \to \mathbb{R}^+$ is given by $g \circ f(x) = e^{-2x}$ for all $x \in \mathbb{R}$. [2 marks]

This function is surjective because for all $y \in \mathbb{R}^+$, $y = g \circ f(-\frac{1}{2}(\ln y))$. [2 marks]

B6. Feedback Part (i) was done correctly more often than not, still in most cases the definition was not completely rigorous, but some leniency was shown when marking. The most common mistake in (ii) was trying to work backwards in the inductive step, in the sense that the student started from $P(k+1)$ and did some manipulations to get to $P(k)$, usually despite having assumed $P(k)$ to be true. Finally, part (iii) was done reasonably well, the most common mistakes were writing the wrong domain/codomain and failing to justify why the composition was surjective.

B7.

(i) Define what it means to say that a set is denumerable. Prove that the set of even integers is denumerable. [3 marks]

(ii) Define what it means for two sets to be equipotent.

Let A, B and C be sets. Prove that if A and B are equipotent and B and C are equipotent, then A and C are equipotent. (You should state, without proof, any properties of functions you use.)

Prove that the open intervals $(0, 1)$ and $(0, 10)$, subsets of the set of real numbers, are equipotent. [5 marks]

(iii) Write the repeating decimal $0.3\overline{457}$ as $\frac{m}{n}$ where m, n are integers. [2 marks]

B7. Solution (i) ILO4 at low and high level, (ii) ILO4 at low level, ILO6 at high level, (iii) ILO4 at medium level.

(i) A set A is denumerable if there exists a bijection $f : \mathbb{N} \to A$. [1 mark]

Let $A = \{2k : k \in \mathbb{Z}\}$. Define $f : \mathbb{N} \to A$ by

$$f(n) = \begin{cases} n, & \text{if } n \text{ is even,} \\ -(n-1), & \text{if } n \text{ is odd} \end{cases}$$

Then f is a bijection because it has inverse $f^{-1} : A \to \mathbb{N}$ given by

$$f^{-1}(2k) = \begin{cases} 2k, & \text{if } k > 0 \\ -2k+1, & \text{if } k \leq 0 \end{cases}$$

By definition A is denumerable. [2 marks]

(ii) Two sets A and B are equipotent if there exists a bijection $f : A \to B$. [1 mark]

Assume A and B are equipotent and B and C are equipotent. Then there exist bijections $f : A \to B$ and $g : B \to C$. Since the composition of two bijections is a bijection, the function $g \circ f : A \to C$ is a bijection and by definition A and C are equipotent. [2 marks]

Let $f : (0, 1) \to (0, 10)$ be defined by $f(x) = 10x$. Then f is a bijection with inverse $f^{-1} : (0, 10) \to (0, 1)$ given by $f^{-1}(x) = \frac{x}{10}$. By definition $(0, 1)$ and $(0, 10)$ are equipotent. [2 marks]

(iii) Let $x = 0.3\overline{457}$. Then

$$10^3 x - x = 345.7\overline{457} - 0.3\overline{457} = 345.4.$$

Therefore $x = \dfrac{3454}{9990}$. [2 marks]

B7. Feedback. (i) Most people stated the correct definition of a denumerable set. To show the set of even integers is denumerable it was enough to provide a bijective correspondence with the natural numbers either using a formula or a description of how the even integers can be listed. Mistakes included only showing the positive even integers are denumerable or showing the even integers are equipotent with the integers.

(ii) Many people had not learned the definition of equipotent sets and instead gave the definition of two sets being equal or an equivalence relation. This meant the rest of part (ii) was incorrect as well. It was not enough to say the sets have the same cardinality without explaining what this means for infinite sets. For the second part a mark was lost if an assumption was made that the sets were finite. For the final part both marks were awarded only if it was demonstrated that there is a bijection between (1,0) and (0,10), rather than simply stating this.

(iii) Most people answered this correctly, however some people answered the wrong question. A mark was awarded for using the correct method.

B8. Let $(x_0, y_0) \in \mathbb{Z}^2$ be an integer solution of the equation $ax + by = c$ where a, b, c are integers.

(i) Assuming that $a \neq 0$ and $b \neq 0$, prove that if $(x, y) \in \mathbb{Z}^2$ is a solution of this equation, then

$$(x, y) = \big(x_0 - \frac{b}{\gcd(a,b)}t,\ y_0 + \frac{a}{\gcd(a,b)}t\big)$$

for some $t \in \mathbb{Z}$. Results from the course used in the proof must be stated, but you do not have to prove them. [6 marks]

(ii) Now assume that $a = 0$ and $b \neq 0$. Is it still true that if $(x, y) \in \mathbb{Z}^2$ is a solution of the equation $ax + by = c$, then (x, y) is given by the formula from (i)? Justify your answer. [4 marks]

B8. Solution ILO7, high level

(i) Assume $a \neq 0$, $b \neq 0$ and denote $\gcd(a, b)$ by d. Assume that $(x, y) \in \mathbb{Z}^2$ is a solution. This means that $ax + by = c$. We are given that (x_0, y_0) is a solution, meaning that $ax_0 + by_0 = c$. Hence $ax + by = ax_0 + by_0$, or equivalently $a(x - x_0) = -b(y - y_0)$.

By definition of gcd, $d \neq 0$ as long as $(a, b) \neq (0, 0)$, hence we can divide through by d and obtain an equivalent equation $\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$. Since $x - x_0$ is an integer, it follows that $\frac{a}{d}$ divides $\frac{b}{d}(y - y_0)$.

We use the following result from the course: if $d = \gcd(a, b)$ then $\frac{a}{d}$ is coprime to $\frac{b}{d}$. We also use the result that whenever k divides ℓm and k is coprime to ℓ, k must divide m. From these two results we conclude that $\frac{a}{d}$ divides $y - y_0$, in other words, $y - y_0 = \frac{a}{d}t$ for some $t \in \mathbb{Z}$.

Then $\frac{a}{d}(x - x_0) = -\frac{b}{d}\frac{a}{d}t$ which implies $x - x_0 = -\frac{b}{d}t$ since a is non-zero. Thus, (x, y) is indeed as stated in the formula. [6 marks]

(ii) It is still true that when $a = 0$, $b \neq 0$, all integer solutions of the equation $ax + by = c$ are of the form given in (i). To see this, observe that the equation becomes $0x + by = c$. It was shown in the course that $\gcd(0, b) = |b|$. Moreover, we are given that (x_0, y_0) is a solution, hence $by_0 = c$ and $y_0 = \frac{c}{b}$, which must therefore be an integer. So the formula from (i) reads

$$\big(x_0 - \frac{b}{|b|}t,\ \frac{c}{b}\big), \quad t \in \mathbb{Z}.$$

Now assume that $(x, y) \in \mathbb{Z}^2$ is a solution. Then x is an integer and $y = \frac{c}{b}$. Putting $t = \frac{|b|}{b}(x_0 - x)$, which is an integer because $\frac{|b|}{b}$ is 1 or -1, ensures that $x = x_0 - \frac{b}{|b|}t$. Thus, (x, y) is still given by the same formula. [4 marks]

Alternatively, full marks could be obtained by modifying the above proof of (i) so as not to use the condition $a \neq 0$. We do not give this alternative solution here.

B8. Feedback B8 turned out to be the most difficult question on the paper. Despite being a "straight bookwork" question, (i) was not done well. During the semester, the students clearly demonstrated that they were able to solve Diophantine equations. The question, however, required justifying the formulaic approach rather than using it, and this proved challenging. The lesson to be learned is that the Foundations course should be about learning to construct an argument, not applying a formula; this will be highlighted more in the subsequent versions of the course.

In (ii), many students claimed that $\gcd(0, b) = b$ rather than $|b|$, but this was immaterial and the students were not penalised for this.

B9. Let the relation $\sim$ be defined on the set $\mathbb{Z}$ as follows: for $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $4\,|(7a^3 + b^3)$.

(i) Prove that $\sim$ is an equivalence relation. [5 marks]

(ii) Show that the equivalence class of the integer 0 is the set of even integers. [3 marks]

(iii) Write down, without proof, one other equivalence class induced by the relation $\sim$. [2 marks]

B9. Solution ILO3 at a medium level, ILO6 at medium (i,ii)/high (iii) level, ILO8 at a medium level.

(i) We show that $\sim$ is **reflexive**, that is, $a \sim a$ for every $a \in \mathbb{Z}$. Indeed, by definition of $\sim$, the statement $a \sim a$ is equivalent to $4\,|(7a^3 + a^3)$, same as $4\,|\,8a^3$. Since $8a^3 = 4 \times 2a^3$, the statement is true by definition of $|$ for all $a \in \mathbb{Z}$. [1 mark]

We show that $\sim$ is **symmetric**, that is, $a \sim b$ implies $b \sim a$. Assume that $a \sim b$, meaning that $7a^3 + b^3 = 4k$ for some integer k. Then $7b^3 + a^3 = 8(a^3 + b^3) - (7a^3 + b^3) = 4(2a^3 + 2b^3 - k)$ is also divisible by 4. This proves that $b \sim a$. [2 marks]

We show that $\sim$ is **transitive**, that is, $a \sim b$ and $b \sim c$ implies $a \sim c$. Assume $a \sim b$ and $b \sim c$, which translates as $7a^3 + b^3 = 4k$ and $7b^3 + c^3 = 4\ell$ for some $k, \ell \in \mathbb{Z}$. Adding these two equations together, we obtain $7a^3 + 8b^3 + c^3 = 4(k + \ell)$, which implies that $7a^3 + c^3 = 4(k + \ell - 2b^3)$ is divisible by 4, so that $a \sim c$. Transitivity is proved. [2 marks]

By definition, a relation which is reflexive, symmetric and transitive, is an equivalence relation.

Alternatively, one could start the solution of (i) by showing that $a \sim b$ is equivalent to $a^3 \equiv b^3 \mod 4$, and prove reflexivity, symmetry and transitivity using congruences. We do not give this alternative solution here.

(ii) By definition, the equivalence class of 0 is the set of all $b \in \mathbb{Z}$ such that $0 \sim b$, that is, $4\,|\,b^3$.

- If b is even, $b = 2\ell$ with $\ell \in \mathbb{Z}$, then $b^3 = 8\ell^3 = 4 \times 2\ell^3$ so by the above $b \sim 0$.
- If b is odd, then b^3 is also odd hence not divisible by 4, so by the above $b \not\sim 0$.

We proved that $b \sim 0$ if and only if b is even, as required. [3 marks]

(iii) For example, the set $\{4k + 1 : k \in \mathbb{Z}\}$, that is, the set of all integers which are congruent to 1 modulo 4, is an equivalence class. [2 marks]

Proof (*not required*): we show that this is the set of all integers equivalent to 1. By definition, $1 \sim b$ if and only if $7 + b^3 \equiv 0 \mod 4$, equivalently $b^3 \equiv 1 \mod 4$. The following table shows that such b are exactly the integers congruent to 1 mod 4:

$b \mod 4$	0	1	2	3
$b^3 \mod 4$	0	1	0	3

One can also observe that $\{4k + 3 : k \in \mathbb{Z}\}$ is an equivalence class. It is the equivalence class of 3.

B9. Feedback The question was well attempted, and part (i) was generally done well. Students were able to demonstrate the knowledge of the three properties required for $\sim$ to be an equivalemce relation. Sometimes, the names of the three properties were mixed up — a lenient approach was taken to this, but of course professional mathematicians should know reflexivity, symmetry and transitivity well. Mistakes that were penalised included proofs of these properties "by example": remember, you must prove that

$a \sim b$ implies $b \sim a$ *for all* $a, b \in \mathbb{Z}$ so it incorrect to only pick, say, $a = 0$ and $b = 2$ and to check that $0 \sim 2 \implies 2 \sim 0$.

Part (ii) tested whether the students could correctly prove equality of two sets, just as in A2(i). Unfortunately, many students proved only one of the two inclusions: $[0] \subseteq 2\mathbb{Z}$ or $2\mathbb{Z} \subseteq [0]$ where $[0]$ denotes the equivalence class of 0, and $2\mathbb{Z}$ denotes the set of even integers. Often this was because the students reasoned using implications, $\implies$, rather than equivalences, $\iff$. It is crucial to understand that equality of sets means two inclusions, and marks were strictly deducted unless the argument was complete.

In part (iii), a number of students simply wrote $[1]$, but, while not incorrect, this answer was not considered fully satisfactory and it was decided that it was fair to give only 1 mark unless the set was written in a more explicit form.

B10.

(i) Give the definition of a prime number.

Deduce from the definition that every prime number p has the following property: for all integers a, a is divisible by p or a is coprime to p.

Is there any non-prime number $p \in \mathbb{N}$ which has this property? Explain your answer.

[5 marks]

(ii) Let P be the set of all prime numbers. Prove: $\exists S \subseteq P$, $1 \leqslant |S| \leqslant 2^{99}$, $\left(\prod_{p \in S} p\right) \equiv 1 \mod 2^{99}$.

[5 marks]

B10. Solution (i) ILO9 at a medium level. (ii) ILO1, ILO5, ILO9 at a medium level, ILO8 and ILO10 at a high level.

(i) A number $p \in \mathbb{N}$ is prime, if p has exactly two positive divisors, namely 1 and p. [2 marks]

Let p be a prime and $a \in \mathbb{Z}$. If $p \,|\, a$, then the required statement is true, so we assume that $p \nmid a$ and prove that a is coprime to p. By definition of a prime number, the positive divisors of p are 1 and p. Out of these, p is not a divisor of a by assumption, hence the only common positive divisor of a and p is 1, and so the greatest common divisor of a and p is 1. This means that a is coprime to p by definition. [2 marks]

Yes, there is a non-prime number, 1, which has the same property. Indeed, for all integers a, a is divisible by 1 (and a is coprime to 1 as well). [1 mark]

(ii) Let $m = 2^{99}$. **Solution 1:** We know from the course that P is an infinite set, hence we can pick m distinct primes $p_1, \ldots, p_m \in P$, none of which equals 2. The set $\{p_1,\, p_1p_2,\, \ldots,\, \ldots,\, p_1p_2 \ldots p_m\}$ has m elements, and the function f, $f(a) = [a]_m$ maps them to non-zero residue classes $[1]_m, \ldots, [m-1]_m$ modulo m: $[0]_m$ cannot occur since none of the elements is even, let alone divisible by m. There are m products but only $m-1$ residue classes, so by the Pigeonhole Principle, f is not injective, and two products are in the same residue class: say,

$$[p_1p_2 \ldots p_k]_m = [p_1p_2 \ldots p_\ell]_m, \quad \text{where } 1 \leq k < \ell \leq m.$$

Note that $p_1 \ldots p_k$ is invertible mod m, as all the p_i are coprime to m. Therefore, $1 \equiv p_{k+1} \ldots p_\ell \mod m$, and we can put $S = \{p_{k+1}, \ldots, p_\ell\}$. [5 marks]

Solution 2 (using Euler's Theorem): There is a residue class mod m which contains infinitely many primes: indeed, if every one of the m classes contained finitely many primes, the union of the classes, $\mathbb{Z}$, would contain finitely many primes — a contradiction. Let these primes be

$$q_1, q_2, q_3, \ldots \in P \cap [a]_m.$$

Then $\gcd(a, m) = 1$ as all these primes must be odd: the only congruence class which contains an even prime is $[2]_m$ but it contains only one prime. Hence by Euler's Theorem, $[a]_m^{\phi(m)} = [1]_m$, so $q_1q_2 \ldots q_{\phi(m)} \equiv 1 \mod m$. Put $S = \{q_1, q_2, \ldots, q_{\phi(m)}\}$, observing that $1 \leqslant |S| = \phi(m) \leqslant m$.

Exercise. Modify both solutions slightly to show that the required set S exists with $1 \leqslant |S| \leqslant 2^{98}$.

Remark. The following naïve argument does not work: "*choose S to be the set of prime factors of $2^{99}+1$*". Indeed, the prime factor 3 occurs in $2^{99}+1$ three times, hence $\prod_{p \in S} p$ is less than $2^{99}+1$ and is not congruent to 1 mod 2^{99}.

B10. Feedback (i) was done quite well, and most arguments presented were logically correct. Majority remembered that 1 is not a prime number (nor is it composite).

(ii) was very difficult, as expected. There were arguments along the lines of Solution 1 as well as Solution 2 above. Some partial marks could be had for stating Euler's theorem and credibly observing that it could be applied to solve the question.

The question could also be solved by appealing to much more difficult results from Number Theory, such as for example Dirichlet's Theorem which implies that there exist primes congruent to 1 modulo 2^{99}, so that the set S can consist of just one prime. The same result could be arrived at using Zsigmondy's Theorem. Although at least one student did quote such an advanced theorem, this was not necessary as such results are completely outside the Foundations course.

END OF EXAMINATION PAPER