MT181 Number Systems: Sheet 1

Attempt all numbered questions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed in at the lecture on Tuesday 7th October.

1. Read the preface and Chapter 1 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. Let $U = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and let

$$X = \{1, 3, 5, 7\}, \quad Y = \{2, 3, 6, 7\}, \quad Z = \{4, 5, 6, 7\}.$$

(a) Draw a Venn diagram showing X, Y, Z as subsets of U. (A suitable configuration of circles is overleaf.)

(b) Write down the members of $(X \cup Y) \cap Z$.

(c) Express each of the sets

$$\text{(i) } \{3, 7\}, \quad \text{(ii) } \{7\}, \quad \text{(iii) } \{3, 4, 5, 6, 7\}, \quad \text{(iv) } \{3, 5, 6, 7\}$$

in terms of X, Y and Z using only intersection $\cap$ and union $\cup$. (You may also use brackets, as in (b), to make clear the order of operations.)

(d) Write down the members of X', the complement of X in U.

(e) Express the set $\{1, 2, 4\}$ in terms of X, Y and Z using intersection $\cap$, union $\cup$, and complements in U.

3. Give 'Yes' or 'No' answers to the following questions. If the answer is 'Yes' give a short justification. If it is 'No', show this by giving an appropriate example.

Let $X = \{\ldots, -3, 1, 1, 3, \ldots\}$ be the set of odd integers.

(a) Is X closed under addition?

(b) Is X closed under multiplication? [*Hint: for a rigorous proof, use that* $x \in X$ *if and only if* $x = 2m+1$ *for some* $m \in \mathbb{Z}$. *Write* $x = 2m+1$ *and* $y = 2n+1$, *where* m, $n \in \mathbb{Z}$, *and multiply out* xy *...*]

Let $\mathbb{Q}_{<0}$ be the set of rational numbers x such that $x < 0$.

(c) Is $\mathbb{Q}_{<0}$ closed under addition? [*Hint: you may assume the result from the second lecture that* $\mathbb{Q}$ *is closed under addition.*]

(d) Is $\mathbb{Q}_{<0}$ closed under multiplication?

(e) Write down an equation that has a solution in $\mathbb{Q}$ but no solutions in $\mathbb{Q}_{<0}$.

4. (a) Find all solutions $x \in \mathbb{R}$, $y \in \mathbb{R}$ to the simultaneous equations $2x + 3y = 18$, $x^2 + y^2 = 25$. [*Hint:* substitute $y = 6 - 2x/3$ into the second equation.]

(b) Find all solutions $x \in \mathbb{R}$, $y \in \mathbb{R}$ to the simultaneous equations $2x + 3y = 18$, $y = 2\sqrt{x+1}$.

[*Note:* If $t \in \mathbb{R}$ and $t \geq 0$ then, by definition, $\sqrt{t}$ is the positive square-root of t. For example $\sqrt{9} = 3$ and $\sqrt{0} = 0$.]

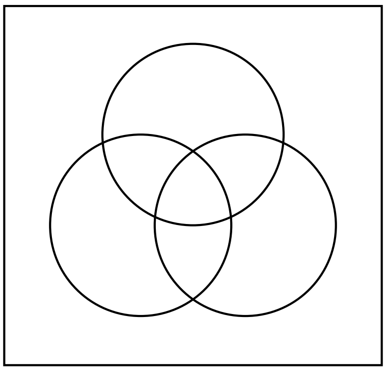
5. Prove the second of De Morgan's laws: if X and Y are subsets of a set U, and complements are taken in U, then $(X \cap Y)' = X' \cup Y'$.

Bonus question: a pond has by 30 fish: 15 are red, 7 are blue and 8 are green. Whenever two fish of different colours meet they each change into fish of the third colour. Whenever two fish of the same colour meet, they change into fish of each of the two other colours.

(For example, if a red and green fish meet, they both become blue, and if two red fish meet, then one becomes blue and the other green.)

It is possible that on some day, all the fish will be red?

Venn diagram for three sets



MT181 Number Systems: Sheet 2

Attempt all numbered questions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

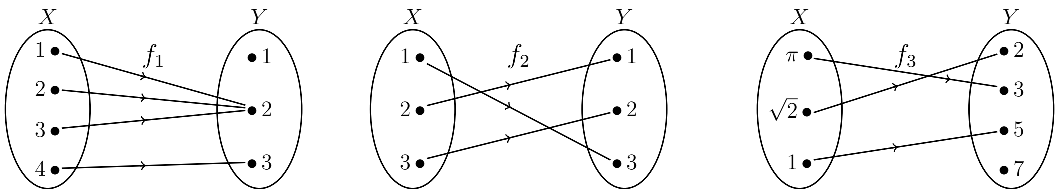
To be handed it at the lecture on Tuesday 14th October.

1. Read Chapters 2 and 3 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. For each of the functions f_1, f_2, f_3 shown as a diagram below:

(i) State its domain, codomain and range.

(ii) State which combination of the properties injective, surjective, bijective it has. Give brief reasons for your answers.



3. The *floor function* $f : \mathbb{R} \to \mathbb{Z}$ is defined so that $f(x)$ is the greatest integer n such that $n \le x$. For example, $f(\pi) = 3$ and $f(1) = 1$.

(a) Write down (i) $f(\sqrt{2})$, (ii) $f(-1/2)$. (Be careful!)

(b) Sketch the graph of the floor function.

(c) Is the floor function (i) injective, (ii) surjective? Give brief reasons.

(The standard notation for the floor of x is $\lfloor x \rfloor$. Please use this if you prefer.)

4. Let $X = \{x \in \mathbb{R} : x \neq 0 \text{ and } x \neq 1\}$. Let $f : X \to X$ be the function defined by

$$f(x) = \frac{1}{1-x}$$

(a) Show that f is bijective and find a formula for $f^{-1} : X \to X$.

(b) Let $g : X \to X$ be the function defined by $g(x) = 1/x$. Simplifying your answers as much possible, find

$$\text{(i) } f\big(f(x)\big), \quad \text{(ii) } f\big(g(x)\big) \quad \text{(iii) } g\big(f(g(x))\big), \quad \text{(iv) } f\big(f(f(x))\big).$$

(c) How many distinct functions can you make by composing f and g in any order?

5. Let X, Y and Z be sets and let $f : X \to Y$ and $g : Y \to Z$ be functions.

(a) Show that if f and g are surjective then gf is surjective.

(b) Show that if gf is surjective then g is surjective.

(c) Give an example where gf is surjective but f is not surjective.

Bonus question: A horizontal stick is one metre long. Fifty ants are placed in random positions on the stick, pointing in random directions. The ants crawl head first along the stick, moving at one metre per minute. If an ant reaches the end of the stick, it falls off. If two ants meet, they both change direction. How long do you have to wait to be sure that all the ants have fallen off the stick?

MT181 Number Systems: Sheet 3

Attempt all numbered questions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 21st October.

1. Read Chapter 4 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009). Try to put into practice the advice in Chapters 3 and 4 when you write your answers to this problem sheet.

2. Write the following complex numbers in the Cartesian form $a + bi$ and plot them on an Argand diagram.

(a) $z_1 = (4 + 3i) + (1 + i)$

(b) $z_2 = (4 + 3i) - (1 + i)$

(c) $z_3 = (4 + 3i)(1 + i)$

(d) $z_4 = (4 + 3i)/(1 + i)$.

3. Find, in Cartesian form, the solutions to the following equations:

(a) $2z + (3 - 3i) = 1 - i$

(b) $(1 + 3i)w + (1 + i) = 3 + 2i$.

Express your solution to (a) in polar form.

4. Let

$$S = \{a + bi\sqrt{3} : a, b \in \mathbb{Q}\}.$$

For example $\frac{1}{3} + 2i\sqrt{3}$ is an element of S, since $\frac{1}{3}$ and 2 are rational numbers.

(a) Show that S is closed under multiplication.

(b) Let $z = a + bi\sqrt{3}$ where $a, b \in \mathbb{Q}$. Suppose that $z \neq 0$. Show that $\mathrm{Re}(1/z) = a/(a^2 + 3b^2)$ and find $\mathrm{Im}(1/z)$. Hence show that $1/z \in S$.

(c) Using (a) and (b) show that S is closed under division.

5. Let φ be the angle such that $0 < \varphi < \pi/2$ and $\tan\varphi = 3/4$. For each of the following complex numbers, find $|z|$ and $\mathrm{Arg}(z)$, writing $\mathrm{Arg}(z)$ in terms of φ and π.

$$\text{(a) } z = 4 + 3i, \quad \text{(b) } z = -1 - 3i/4, \quad \text{(c) } z = -3 + 4i.$$

6. Find the complex numbers (a) 1, (b) i, (c) i^2, (d) i^3, (e) i^4 in Cartesian form. Hence find i^{2013} in Cartesian form. Justify your answer.

Bonus question A: Consider this chain of claimed equalities:

$$-1 = \sqrt{-1}^{\,2} = \sqrt{-1}\sqrt{-1} = \sqrt{(-1)^2} = \sqrt{1} = 1.$$

Where is the mistake?

Bonus question B: Do there exist irrational real numbers x and y such that $x^y \in \mathbb{Q}$? [*Hint:* consider $x = \sqrt{2}^{\sqrt{2}}$ and $x^{\sqrt{2}}$.]

MT181 Number Systems: Sheet 4

Attempt all numbered questions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 28th October.

1. Read Chapter 5 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. Write the complex numbers $z = 2 - 2i$ and $w = 4i$ in exponential form.

3. (a) Find all solutions $z \in \mathbb{C}$ to the equation $z^6 = 1$ in exponential form.

(b) Express each solution in Cartesian form.

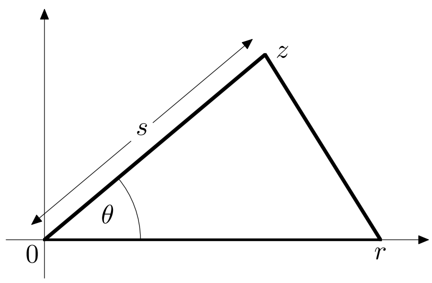
(c) Plot the solutions on an Argand diagram.

4. Let $C = \{z \in \mathbb{C} : |z - 1| = 2\}$. Let $D = \{z \in \mathbb{C} : |z + 1| = 2\}$.

(a) Plot C and D on an Argand diagram. [*Hint:* $|z - 1| = 2 \iff$ the distance between z and 1 is 2.]

(b) Express the elements of $C \cap D$ in Cartesian form.

5. The Argand diagram below shows a triangle with vertices at 0, $r \in \mathbb{R}$ and $z \in \mathbb{C}$. Let s be the length of the side with vertices at 0 and z and let θ be the marked angle.



(a) Express the lengths of the other two sides of the triangle in terms of r and z. [*Hint:* for the side from r to z, Question 4(a) has a relevant idea.]

(b) Show that $z + \overline{z} = 2s\cos\theta$. [*Hint:* what is z in polar form?]

(c) By expanding $|z - r|^2 = (z - r)\overline{(z - r)}$ prove the cosine rule.

6. Let $a, b, c, d \in \mathbb{R}$. Let

$$z = (a + bi)(a - bi)(c + di)(c - di).$$

(a) Show that $z = (a^2 + b^2)(c^2 + d^2)$.

(b) By reordering the factors in the product defining z and then multiplying out, show that $z = (ac - bd)^2 + (ad + bc)^2$.

(c) Given that $137 = 4^2 + 11^2$ and $149 = 7^2 + 10^2$, find *natural numbers* r and s such that

$$r^2 + s^2 = 137 \times 149.$$

(d) (Optional.) State and prove a generalization of (c).

Bonus question: You and two of your friends are on your way to a party. At the party, a white or black hat will be put on each person's head. You will be able to see your friends' hats, but not your own.

When the host says 'Go!' you may stay silent, or say either 'White' or 'Black'. Then

- if at least one person speaks, and everyone who speaks says the colour of their own hat, you all get some cake;
- if anyone says the opposite colour to their own hat, or everyone stays silent, there is no cake.

Everyone who speaks must speak at the same time: you may not wait to hear what one of your friends says before deciding whether to speak. You must not speak after the hats are put on, except as permitted above.

Before the hats are put on, you have a few minutes to agree a strategy with your friends. Find a good strategy.

MT181 Number Systems: Sheet 5

Attempt all numbered questions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 4th November.

1. Read Chapter 24 on induction of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. Find the complex numbers z that satisfy the equation $z^2 - (6+2i)z + 8 + 2i = 0$. Write your solutions in the form $a + bi$ where a, $b \in \mathbb{R}$.

3. Solve the equation $\mathrm{e}^z = 1 + i$. [*Hint:* start by writing $1 + i$ in exponential form. Make sure to give all solutions.]

4. We have defined the complex exponential function by $\exp(a+bi) = \mathrm{e}^a(\cos b + i \sin b)$ for a, $b \in \mathbb{R}$. For $w \in \mathbb{C}$, it was shown in lectures that the equation $\exp z = w$ has a solution $\iff w \neq 0$.

(a) Is exp surjective? Justify your answer.

(b) Is exp injective? Justify your answer.

(c) Let $L = \{z \in \mathbb{C} : \operatorname{Re} z = 2\}$. Draw $\{\exp z : z \in L\}$ on an Argand diagram.

(d) Define a subset X of $\mathbb{C}$ such that $\exp : X \to \{w \in \mathbb{C} : w \neq 0\}$ is bijective.

5. (a) Calculate $\sum_{k=1}^{n} k^3$ for $n = 1, 2, 3, 4, 5$.

(b) Conjecture a formula for $\sum_{k=1}^{n} k^3$.

(c) Prove your formula by induction on n.

[*Hint: to spot the pattern try taking squareroots of the numbers you found in (a). You may assume the result in Example 4.3.*]

6. Use the Principle of Mathematical Induction to show that

(a) $4^n + 5$ is a multiple of 3 for all $n \in \mathbb{N}$.

(b) $2^n \geq 6n$ for all integers n such that $n \geq 5$.

7. Let $n \in \mathbb{N}$ and let $z \in \mathbb{C}$.

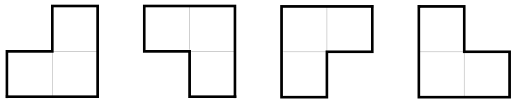
(a) Express $1 + 2z + 3z^2 + 4z^3 + \cdots + (n+1)z^n$ using Sigma notation.

(b) Write $\sum_{k=0}^{n} 3^k$ using the $\cdots$ notation.

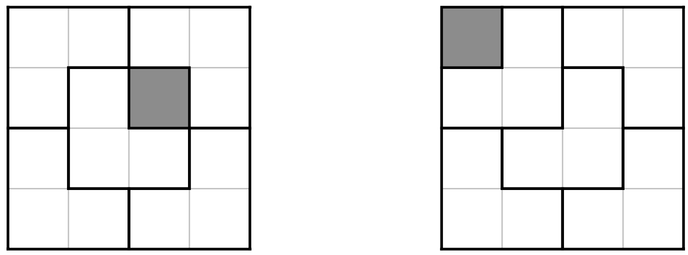
(c) Simplify $\sum_{j=0}^{n-1} (z+j)^j - \sum_{k=1}^{n} (z+k)^k$.

(d) Simplify $\sum_{j=1}^{n} z^j - \sum_{j=1}^{n+1} z^{j-1}$.

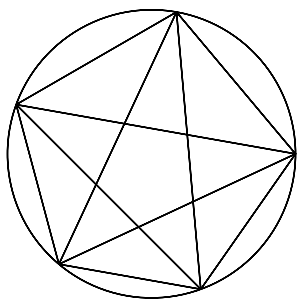
Bonus question 1: You are given a $2^n \times 2^n$ board with one square missing. Show that, no matter which square is missing, it is always possible to tile the board with L-shaped pieces, as shown below.



Two example tilings of 4×4 boards are shown below.



Bonus question 2: Let a_n be the maximum number of regions that can be formed by taking n points on the circumference of a circle, and joining them all up by straight lines. (Do not count the region outside the circle.) For example, the diagram below shows that $a_5 = 16$.



Find a_1, a_2, a_3 and a_4. Make a conjecture about the general pattern. Now test your conjecture by finding a_6.

Make a table showing the differences $a_n - a_{n-1}$, then the second differences, $(a_n - a_{n-1}) - (a_{n-1} - a_{n-2})$, and so on. Use your table to guess a_7. It might help to include the value $a_0 = 1$.

This problem is like Example 4.2: both show the danger of jumping to conclusions from small cases.

MT181 Number Systems: Sheet 6

Attempt all numbered questions: 6(e) is optional. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 11th November.

1. Read Chapters 15 and 16 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. Prove by induction that the minimum number of moves needed to move n discs from one peg to another in the Towers of Hanoi Problem is $2^n - 1$. [*Hint:* you may assume the result proved in lectures that $2^n - 1$ moves suffice.]

3. Find the quotient and remainder when n is divided by m in each of these cases:

(i) $n = 42$, $m = 8$ (ii) $n = 43$, $m = 8$ (iii) $n = 8$, $m = 43$ (iv) $n = -43$, $m = 8$.

4. Let m, $n \in \mathbb{N}$. Suppose that when $m, n \in \mathbb{N}$ are divided by 4 they both have remainder 3. What is the remainder when mn is divided by 4?

5. (a) Let n, r and s be natural numbers all greater than 1 such that

$$n = rs \quad \text{and} \quad r \leq s.$$

By supposing that $r > \sqrt{n}$ and deriving a contradiction, show that $r \leq \sqrt{n}$.

(b) Deduce that if n is a composite number then n is divisible by a prime p such that $p \leq \sqrt{n}$.

(c) Find the prime factorizations of 1327 and 2662.

6. Define a function $d : \mathbb{N} \to \mathbb{N}$ so that $d(n)$ is the number of natural numbers m such that n is divisible by m. For example, 12 is divisible by 1, 2, 3, 4, 6 and 12, so $d(12) = 6$.

(a) Find $d(26)$ and $d(27)$.

(b) Make a table showing $d(n)$ for each n between 1 and 18.

(c) Complete the following proposition $d(n) = 2 \iff n$ is ...

(d) Describe in terms of their prime factorizations, the natural numbers n such that (i) $d(n) = 3$ and (ii) $d(n) = 4$. [*Hint:* use $\iff$ as in (c).]

(e) ($\star$) Prove your answers to (d) are correct.

7. (a) By adapting the proof of Claim 5.10, prove that $\sqrt[3]{5}$ is irrational.

(b) Write down a proposition that generalizes the result proved in (a). [*Hint:* the end of Chapter 16 of *How to think like a mathematician* may be helpful.]

Bonus question A: The 100 lights in the main lecture theatre at the University of Erewhon are controlled by a switchboard with switches numbered from 1 to 100. Each morning at 8am, all the switches are set to off. Then

Every even numbered switch is flipped,

Every switch whose number is divisible by 3 is flipped,

Every switch whose number is divisible by 4 is flipped,

Every switch whose number is divisible by 5 is flipped,

$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \; \vdots \; \vdots \quad \vdots$

Every switch whose number is divisible by 100 is flipped.

The process is completed by 8.59am. Which lights are on during the 9am lecture?

Bonus question B: Is there a polynomial $f(x)$ with coefficients in the integers such that $f(a) = b$, $f(b) = c$ and $f(c) = a$ for distinct $a, b, c \in \mathbb{N}$? (For a hint, see page 162 of Liebeck, *A concise introduction to pure mathematics*.)

MT181 Number Systems: Sheet 7

Attempt all the numbered questions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 18th November.

1. Read Chapters 6 and 7 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. A proposition is said to be a *tautology* if it is always true. Which of the following are tautologies? Justify your answers.

(a) $(P \implies Q) \iff (\neg P \vee Q)$,

(b) $\neg(P \wedge Q) \iff \neg P \wedge \neg Q$,

(c) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$,

(d) $(P \implies Q) \implies (Q \implies P)$,

(e) $\big((P \Longrightarrow Q) \Longrightarrow R\big) \Longrightarrow (Q \Longrightarrow R)$,

(f) $\big((P \Longrightarrow Q) \wedge (Q \Longrightarrow R)\big) \Longrightarrow (P \Longrightarrow R)$.

[*Hint:* You can use truth tables, or argue directly, as you prefer. The direct proofs are usually shorter. If you use truth tables you will need eight rows for (e) and (f).]

3. Let X, Y and Z be sets and let $f : X \to Y$ and $g : Y \to Z$ be functions. Decide whether the following propositions are true or false. Justify your answers with a proof or an explicit counterexample, as appropriate.

(a) (f injective $\wedge$ g injective) $\implies$ gf injective,

(b) gf injective $\implies$ (f injective $\wedge$ g injective).

4. One day you meet three people, A, B and C. You know that one is a *Knight*, who always tell the truth, one is a *Knave*, who always lies, and the other is a *Spy*, who answers as he sees fit. You hear the following.

A says to B: 'I have heard you lie today'

B says to C: 'You are a knight'

C says to A: 'I have heard you tell the truth today'

State the identity of each person. [*Hint:* you could try all possibilities but there are faster arguments.]

5. There are eight truth tables of the form below, where each of the starred entries is either true or false. (For example, one has entries T, T, T, F read from top to bottom, another has entries F, T, T, F, and so on.)

P	Q	
T	T	$\star$
T	F	$\star$
F	T	$\star$
F	F	F

For each such table, write down a proposition having that truth table. Use only parentheses and the symbols $P, Q, \vee, \wedge$ and $\neg$. (You need not use both propositions. You need not use all symbols.)

6. In the language of Erewhon, the words for Yes and No are Bal and Da, but you do not know which way round they are. So *either* Bal means Yes and Da means No, *or* Bal means No and Da means Yes.

You see two people, one of whom is a Knight and the other a Knave, as defined in Question 4. Again you do not know which is which.

(a) Complete the table below showing the answers to the questions

Q: Does Bal mean Yes?

R: Does Bal mean No?

Bal means	Person asked	Q	R
Yes	Knight	Bal	Da
No	Knight		
Yes	Knave		
No	Knave		

(b) Give a single question whose answer will determine which person is the Knight. [*Hint:* use (a).]

(c) Give a single question whose answer will determine the meaning of Bal. (Do not assume you know which person is a Knight.) [*Hint:* find a question to which the Knight and Knave will give the same answer.]

(d) ($\star$ Optional) There are two paths, one leading to the marsh, the other to the beach. What single question can you ask that will determine which path leads to the beach? (For a simpler problem, suppose you know the meaning of Bal, or which person is a Knight.)

Based on Chapter 11 of Raymond Smullyan, *What is the name of this book?*, Penguin 1978.

MT181 Number Systems: Sheet 8

Attempt questions 1 to 6. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 25th November.

1. Read Chapters 10 and 11 on quantifiers of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. State the truth value (true or false) of each of the following propositions.

(i) $\{1, 2\}$ is an element of $\bigl\{\{1, 2\}, 2, 3\bigr\}$,

(ii) $\{1, 2\}$ is a subset of $\bigl\{\{1, 2\}, 2, 3\bigr\}$,

(iii) $\{4, 5\}$ is a subset of $\bigl\{\{4, 5\}, 4, 5, 6\bigr\}$

(iv) $\bigl|\bigl\{\{1, 2\}, 2, 3\bigr\}\bigr| = 4$,

(v) $\bigl|\bigl\{\{4, 5\}, 4, 5, 6\bigr\}\bigr| = 4$.

3. Show that the proposition below is false:

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\mathrm{e}^{a+bi} = 2i \implies a = \ln 2 \text{ and } b = \pi/2).$$

Rewrite the part of the proposition following '$\Longrightarrow$' so that the proposition is correct. [*Hint:* you will need the quantifier $\exists n \in \mathbb{Z}$. **Misprinted as** $\exists n \in \mathbb{N}$**, corrected in lecture on Friday 21st November.**]

4. (a) Let Q be the proposition $(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})(n$ is divisible by $m)$.

(i) Find a proposition logically equivalent to $\neg Q$ that starts $(\exists m \in \mathbb{N})$.

(ii) Is Q true? Explain your answer.

(b) Let R be the proposition $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n$ is divisible by $m)$.

(i) Find a proposition logically equivalent to $\neg R$ that starts $(\forall n \in \mathbb{N})$.

(ii) Is R true? Explain your answer.

5. Let $U = \{1, 2, \ldots, 2014\}$. Define subsets X, Y, Z of U by

$$X = \{n \in U : n \text{ is even}\}$$
$$Y = \{n \in U : n \text{ is divisible by } 3\}$$
$$Z = \{n \in U : n \text{ is divisible by } 5\}$$

(a) Show that if $m \in \mathbb{N}$ then the number of elements of U that are divisible by m is $\lfloor 2014/m \rfloor$, where $\lfloor\ \rfloor$ is the floor function first seen in Question 3 of Sheet 2.

(b) By applying the Principle of Inclusion and Exclusion to the sets X, Y and Z, find the number of elements of U that are *not* divisible by *any* of 2, 3 or 5.

6. (a) How many functions $f : \{1, 2, 3, 4\} \to \{0, 1\}$ are there? [*Hint:* how many choices are there for $f(1)$? How many choices are there for $f(2)$? ...]

(b) Why is the answer to (a) the same as the number of subsets of $\{1, 2, 3, 4\}$?

(c) How many surjective functions $f : \{1, 2, 3, 4\} \to \{0, 1\}$ are there?

(d) Is there an injective function $f : \{1, 2, 3, 4\} \to \{0, 1\}$? Justify your answer.

(e) Write down a generalization of (a).

Bonus question: Six pirates have secured their treasure chest with padlocks, labelled A, B, C, and so on. The chest can only be opened when every single padlock has been unlocked. Each pirate has keys to a subset of the padlocks; for example, one might have keys to padlocks A, C, D, another might have keys to padlocks B, D, E, and so on. The distribution of keys is arranged so that the box can be opened if and only if at least four pirates are present.

The pirates wish to arrive at this situation using as few padlocks as possible. How many padlocks are there on their treasure chest?

MT181 Number Systems: Sheet 9

Attempt questions 1 to 6. Question 7 is optional but recommended for revision on functions. Please staple your answers together and put your name and student number on the top sheet. Do not return the problem sheet.

The lecturer will be happy to discuss any of the questions in office hours.

To be handed it at the lecture on Tuesday 2nd December.

1. Read Chapter 29 on modular arithmetic of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

Houston uses the word 'equivalent' rather than 'congruent', but otherwise his definitions and notation are the same as in lectures.

2. (a) Make a table showing the remainder of 2^n on division by 11 for $n = 0, 1, 2, \ldots, 11, 12$. [*Hint:* if $2^n \equiv r \bmod 11$ then $2^{n+1} \equiv 2r \bmod 11$.]

(b) Find $2^{2014} \bmod 11$.

(c) Find all solutions $n \in \mathbb{N}$ to the equation $2^n \equiv 9 \bmod 11$.

3. (a) Find an integer n such that $0 \leq n < 5$ and $n \equiv 2013 \bmod 5$.

(b) Find an integer n such that $-5 \leq n < 0$ and $n \equiv 2013 \bmod 5$.

(c) Find all integers k such that $2k \equiv 1 \bmod 5$.

(d) Does the congruence $3n \equiv 7 \bmod 9$ have a solution with $n \in \mathbb{Z}$? Justify your answer.

4. The *square code* is defined after Example 8.9 to be

$$\{(u_1, u_2, u_3, u_4, u_1 + u_2, u_3 + u_4, u_1 + u_3, u_2 + u_4) : u_1, u_2, u_3, u_4 \in \{0, 1\}\}$$

where the addition is done mod 2, as in Example 8.9(c). For example $0 + 1 = 1$ and $1 + 1 = 0$. The elements of the square code are called *codewords*.

(a) How many codewords are there in the square code?

(b) Suppose that Alice sends 11000011 and Bob receives 01000011. Bob represents 01000011 by the square

$$\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & 0 \\ \hline 1 & 1 & \end{array}$$

(i) Explain why Bob knows that an error has occurred.

(ii) Suppose Bob assumes that exactly one error has occurred. Explain how Bob can deduce that Alice sent 11000011.

(c) Suppose you receive 00100110, 01001100 and 01101110. In each case decide which codeword in the square code was most probably sent.

5. (a) Use Euclid's algorithm to find the greatest common divisor of 170 and 2921.

(b) Determine $s, t \in \mathbb{Z}$ such that $170s + 2921t = 1$.

(c) Find all $x \in \mathbb{Z}$ such that $170x \equiv 15 \bmod 2921$.

6. Set a question on functions (see Section 2) in the style of previous compulsory problem sheet questions.

Please give the answers to any numerical parts. A full model solution is not required, but you may supply one if you wish. State briefly how hard you think your question is.

7. (a) Let $f : X \to Y$ be a function. What does it mean to say that f is injective?

(b) Let $f : \{x \in \mathbb{R} : x \geq 0\} \to \{x \in \mathbb{R} : x \geq 1\}$ be the function defined by $f(x) = (x+1)^3$.

(i) What is the domain of f? What is the codomain of f?

(ii) Show that f is injective. [*Hint:* A good start to your answer would be 'Suppose that $x, x' \in [0, \infty)$. Then

$$f(x) = f(x') \implies (x+1)^3 = (x'+1)^3 \implies \ldots' .]$$

(iii) Show that f is surjective.

(iv) What are the domain and codomain of the inverse function f^{-1}?

(v) Find a formula for $f^{-1}(y)$ where y is in the domain of f^{-1}.

Bonus question A: find the number of zeros at the end of 2014!.

Bonus question B: a sequence $a_1, a_2, a_3, \ldots$ satisfies the following conditions: (i) $a_n \in \mathbb{N}$ for all $n \in \mathbb{N}$, (ii) $a_m < a_n$ if $m < n$ and (iii) $a_{a_n} = 3n$ for all $n \in \mathbb{N}$. Find a_{2014}.

MT181 Number Systems: Sheet 10

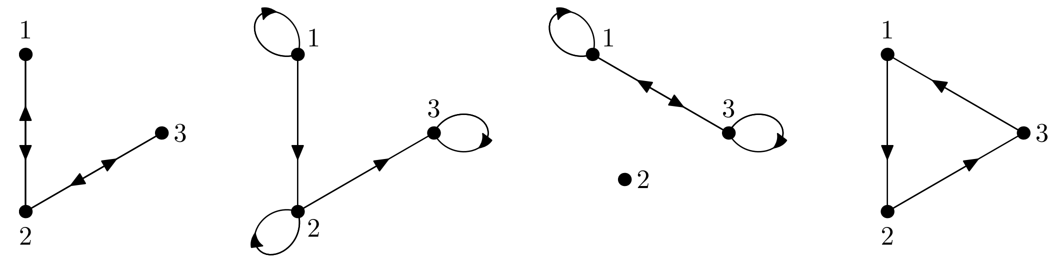
Attempt all numbered questions.

The lecturer will be happy to discuss any of the questions in office hours.

Answers to the first four questions will appear on Moodle on December 9th, and the rest will appear on December 13th. You can get help with this problem sheet in workshops and office hours as usual.

1. Read Chapter 31 on equivalence relations of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. The four diagrams below show relations on the set $\{1, 2, 3\}$: an arrow is drawn from x to y if and only if $x \sim y$. A loop is drawn on x if and only if $x \sim x$.



(a) For each relation state whether it is (i) reflexive, (ii) symmetric, and (iii) transitive. Justify your answers briefly.

(b) Define four further relations on the set $\{1, 2, 3\}$ that have each of the four remaining combinations of the properties reflexive, symmetric and transitive.

3. Define a relation $\sim$ on $\mathbb{C}$ by

$$z \sim w \iff |z| = |w|.$$

(a) Prove that $\sim$ is an equivalence relation.

(b) Draw the equivalence classes $[2i]$, $[e^{i\pi/3}]$ and $[0]$ on an Argand diagram.

4. The following argument claims to show that if $\sim$ is a relation on a set X that is symmetric and transitive then $\sim$ must be reflexive.

> 'Given $x \in X$ choose $y \in X$ such that $x \sim y$. By symmetry $y \sim x$. Hence $x \sim y$ and $y \sim x$, so by transitivity $x \sim x$. Thus $\sim$ is reflexive.'

Where is the flaw in this argument? [*Hint:* Question 2(a) is relevant.]

5. Find the multiplicative inverses of $[10]$ and $[14]$ in $\mathbb{Z}_{37}$.

6. Let $n \in \mathbb{N}$. Suppose that $n = d_k d_{k-1} \ldots d_1 d_0$ in base 10.

(a) Prove that $n \equiv d_0 + d_1 + \cdots + d_k \bmod 9$. Hence show that 9 divides n if and only if 9 divides $d_0 + d_1 + d_2 + \cdots + d_k$.

(b) Prove that 11 divides n if and only if 11 divides $d_0 - d_1 + d_2 - \cdots + (-1)^k d_k$.

(c) Let $n = 123\,456\,789\,123\,456\,789$. Find the remainder when n is divided by 9. Find the remainder when n is divided by 11.

7. (a) Write down addition and multiplication tables for $\mathbb{Z}_6$.

(b) Find all $x \in \mathbb{Z}_6$ such that $[2] \times x = [4]$.

(c) Does $[2]$ have a multiplicative inverse (see Definition 10.2) in $\mathbb{Z}_6$?

8. Let R be a ring. Prove the following parts of Lemma 10.5.

(ii) The one element in R is unique. [*Hint:* suppose that $u, u' \in R$ are such that $ur = u'r = r$ for all $r \in R$. Adapt the proof of Lemma 10.5(i).]

(vii) If $x \in R$ then $-(-x) = x$.

(viii) If $x, y \in R$ then $-(xy) = (-x)y = x(-y)$ and $(-x)(-y) = xy$.

(ix) $0 = 1$ if and only if $R = \{0\}$.

Bear in mind that $-x$ means the element of R given by property (3) which satisfies $-x + x = 0$. Other parts of Lemma 10.5 proved in lectures will be useful.

9. Let R be a finite integral domain. So R is a finite commutative ring such that for all x, $y \in R$,

$$xy = 0 \implies x = 0 \text{ or } y = 0.$$

Show that for each non-zero $x \in R$, the map $f_x : R \to R$ defined by $f_x(y) = xy$ is injective. Hence show that R is a field.

10. Let F be a field. Show that if $g(x) \in F[x]$ has degree d then $g(x)$ has at most d roots in F, counted with multiplicities. [*Hint:* adapt the proof of Corollary 10.15.]

Bonus question: There are 10 pirates who have recently acquired a bag containing 100 gold coins. The leader, number 1, must propose a way to divide up the loot. For instance he might say 'I'll take 55 coins and the rest of you can have five each'. A vote is then taken. If the leader gets *half or more* of the votes (the leader getting one vote himself), the loot is so divided. Otherwise he is made to walk the plank by his dissatisfied subordinates, and number 2 takes over, with the same responsibility to propose an acceptable division.

Assuming that the pirates are all greedy, untrustworthy, and capable mathematicians, what happens? [*Hint:* try thinking about a smaller 2 or 3 pirate problem to get started.]
