MT181 Number Systems: Sheet 1

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 11th October.

1. Read the preface and pages 3–8 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

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. For each set below give 'Yes' or 'No' answers to the questions: (i) is the set closed under addition? and (ii) is the set closed under multiplication? Justify your answers with short explanations or examples as appropriate.

(a) The set $\mathbb{Q}_{>0}$ of rational numbers q such that $q > 0$.

(b) The set $X = \{\ldots, -3, -1, 1, 3, \ldots\}$ of odd integers.

(c) The set $\mathbb{R}_{\leq 0}$ of real numbers that are less than or equal to 0.

(d) The set Y of real numbers r such that $-2 \leq r \leq 2$.

(e) The set Z of complex numbers of the form $a + bi\sqrt{3}$ where $a, b \in \mathbb{Q}$.

4. Find the complex numbers z and w satisfying the following equations:

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

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

5. Let $z = a + bi$ and $w = c + di$ be complex numbers. In lectures it was shown that $\overline{z + w} = \overline{z} + \overline{w}$. Show similarly that $\overline{zw} = \overline{z}\ \overline{w}$ and that $\overline{z/w} = \overline{z}/\overline{w}$.

6. Write the complex number i^{40041} in the form $a + bi$. [*Hint: first write* i^4 *in the form* $a + bi$.]

Bonus question: the pond below Founder's Building is populated by 30 fish: 15 are red, 7 are blue and 8 are green. Whenever two fish of different colours meet, a horrifying transformation occurs, and they each change into fish of the third colour. Whenever two fish of the same colour meet, they change into both of the 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?

MT181 Number Systems: Sheet 2

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 18th October.

1. Read Chapters 2 and 3 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009). Next week there will be an exercise in which you are asked to write out a proof, following the guidelines given in Chapter 3.

2. Write the complex number $z = 2 - 2i$ and $w = -1 - i$ in exponential form.

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

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

4. Let $\mathbf{N}_0$ denote the set $\{0, 1, 2, \ldots\}$ of the natural numbers together with 0.

(a) Suppose that $r = a^2 + b^2$ and $s = c^2 + d^2$ where $a, b, c, d \in \mathbf{N}_0$. By multiplying out the product

$$(a + bi)(a - bi)(c + di)(c - di)$$

in two different ways, show that there exist $x, y \in \mathbf{N}_0$ such that $rs = x^2 + y^2$.

(b) Given that $137 = 4^2 + 11^2$ and $149 = 7^2 + 10^2$, use your solution to (a) to express $137 \times 149 = 20413$ as the sum of two squares of natural numbers.

5. Let $w = \mathrm{e}^{i\pi/3}$.

(a) Show that $w^3 + 1 = (w^2 - w + 1)(w + 1)$. Hence show that $w^2 - w + 1 = 0$.

(b) By solving a quadratic equation show that either $w = \frac{1}{2} + \frac{i\sqrt{3}}{2}$, or $w = \frac{1}{2} - \frac{i\sqrt{3}}{2}$. Which choice is correct? [*Hint:* where, roughly, is w on an Argand diagram?]

(c) Write w in polar form. Deduce that $\cos\frac{\pi}{3} = \frac{1}{2}$ and $\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$.

6. Let X be the set of complex number z of the form $2\mathrm{e}^{i\theta}$, where $-\pi/2 \leq \theta \leq 0$. Plot X on an Argand diagram.

Let Y be the set of complex numbers z such that $|z - (1 + i)| = 1$. Plot Y on an Argand diagram.

7. (a) Find the square roots of i, i.e., find all solutions $z \in \mathbb{C}$ to the equation $z^2 = i$.

(b) Find all solutions $z \in \mathbb{C}$ to the equation $z^5 = 32\mathrm{e}^{5/6\pi i}$ and plot them on an Argand diagram.

Bonus question: do there exist irrational numbers x and y such that x^y is rational. [*Hint:* let $x = \sqrt{2}^{\sqrt{2}}$ and consider x and $x^{\sqrt{2}}$.]

MT181 Number Systems: Sheet 3

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 25th October.

Half of your mark for Question 2 will be given for following the advice in Chapter 3 of *How to think like a mathematician*. So you should write in full sentences, explain what you are doing, use '=' and other symbols correctly, avoid excessive use of arrows, etc.

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

2. Let $s_j = 1 + 3 + 5 + \cdots + (2j - 1)$. Compute s_1, s_2, s_3, s_4 and make a conjecture on the value of s_n for a general $n \in \mathbb{N}$. Prove your conjecture by induction on n.

3. For each of the following statements, write down whether it is a proposition, a predicate, or neither. For each proposition P, state whether P is true or false. For each predicate Q, state whether $Q(3)$ is true or false.

(a) $2 + 2 = 7$

(b) $2^n > n^2$.

(c) For all $n \in \mathbb{N}$, either n is even or n is odd.

(d) If $n \in \mathbb{N}$ then $n^2 + n + 41$ is a prime number.

(e) Prime numbers are nicer than composite numbers.

4. 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 $n \geq 5$.

(c) $\sum_{j=1}^{n} j^3 = \left(\sum_{j=1}^{n} j\right)^2$ for all $n \in \mathbb{N}$. [*Hint:* you may assume Claim 3.5.]

5. Find integers q and r such that $n = qm + r$ where $0 \leq r < m$ when

(a) $n = 34, m = 7$; (b) $n = 7$, $m = 34$; (c) $n = 2012$, $m = 34$.

Find the remainders r when $n = 19$, $m = 7$ and when $n = -19$, $m = 7$. What do you notice about the sum of remainders?

6. Let $n \in \mathbb{N}$ and let $x \in \mathbb{C}$.

(a) Simplify $\sum_{j=0}^{n}(x + j)^j - \sum_{j=0}^{n-1}(x + j)^j$.

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

(c) Express $1 + 2x + 3x^2 + 4x^3 + \cdots + (n + 1)x^n$ in Sigma notation.

Bonus question: A painter has tins containing a litre of red paint and a litre of blue paint. The painter transfers a cupful of blue paint into the red tin, mixes it up thoroughly, and then transfers a cupful of the mixture back into the blue tin. Which is greater: the fraction of blue paint in the red tin, or the fraction of red paint in the blue tin?

MT181 Number Systems: Sheet 4

Attempt questions 1 to 6 and at least one of 7 and 8. To be handed in during the MT181 lecture on Thursday 1st November.

1. Read Chapters 4 and 25 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009)

2. (a) Evaluate $\sum_{j=1}^{3} j(j-1)$.

(b) Prove by induction on n that $\sum_{j=1}^{n} j(j-1) = \frac{n}{3}(n^2-1)$ for all $n \in \mathbb{N}$.

3. Use Euclid's Algorithm to determine $\gcd(m,n)$ and hence to find integers s and t such that $\gcd(m,n) = sm + tn$ when (i) $m = 851$, $n = 391$ and (ii) $m = 61938$, $n = 16983$.

4. Show that the fraction $\dfrac{21n+4}{14n+3}$ is always in lowest terms, for any $n \in \mathbb{N}$. [*Hint:* use Euclid's Algorithm to find the greatest common divisor of $21n+4$ and $14n+3$.]

5. (a) Let n be a composite number. Let p be the smallest prime dividing n. By assuming that $p > \sqrt{n}$ and deriving a contradiction, show that $p \leq \sqrt{n}$.

(b) Using (a) and a calculator show that 1327 is prime and decide whether or not 1331 is prime.

6. Prove that $3^{1/3}$ is irrational.

7. (a) Make a table showing the number of divisors of each natural number between 1 and 16 (go further if you wish). For example, 14 has four divisors, since 14 is divisible by 1, 2, 7 and 14.

(b) Describe, in terms of their prime factorizations, the natural numbers which have (i) exactly one, (ii) exactly two, (iii) exactly three and (iv) exactly four divisors. (Your table should help you to spot a general pattern.)

8. Let S be the set of all natural numbers of the form $4m+1$ where $m \in \mathbb{N}$, so $S = \{5, 9, 13, 17, 21, 25, \ldots\}$.

(a) Prove that S is closed under multiplication.

In the remainder of this question, we say that $n \in S$ is *S-prime* if there do not exist $a, b \in S$ such that $n = ab$.

(b) Show that 21 is S-prime and that 25 is not S-prime.

(c) Prove, by strong induction, that any element of S can be written as a product of S-primes.

(d) Give an example to show that the factorization in (c) is not in general unique.

Bonus question: 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) $a_{a_n} = 3n$ [**not** $3a_n$] for all $n \in \mathbb{N}$. Find a_{2012}.

MT181 Number Systems: Sheet 5

Attempt at least questions 1 to 6. Solutions will be posted on Moodle on Thursday 8th November. There are some revision examples and further questions on complex numbers available from Moodle: see the links for week 3.

1. Read Chapter 5 on problem solving and Chapter 26 on the contrapositive of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009)

2. Let $z = -1 + i\sqrt{3}$.

(a) Draw z on an Argand diagram and find $|z|$ and $\mathrm{Arg}(z)$.

(b) Express z in polar and in exponential form.

(c) Show that $z^3 = 8$.

(d) Find, in Cartesian form, all the complex numbers w such that $w^3 = 8$. [*Hint:* first find the w in exponential form, then convert them to Cartesian form. Problem 2.5 is relevant.]

3. (a) Evaluate $\displaystyle\sum_{j=1}^{2} \frac{j^2}{(2j-1)(2j+1)}$ and $\displaystyle\sum_{j=1}^{3} \frac{j^3}{(2j-1)(2j+1)}$.

(b) Prove by induction that $\displaystyle\sum_{j=1}^{n} \frac{j^2}{(2j-1)(2j+1)} = \frac{n(n+1)}{2(2n+1)}$ for all $n \in \mathbb{N}$.

4. Find the prime factorization of 111111, by testing for divisibility by the odd primes $3, 5, 7, 11, 13, \ldots$ in turn.

5. Let $n \in \mathbb{N}$. Suppose that n has prime factorization $p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ where $p_1, p_2, \ldots, p_r$ are primes and $p_1 < p_2 < \ldots < p_r$.

(a) Show that if a_1, a_2, $\ldots$, a_r are all even then n is a square number.

(b) Show conversely that if n is a square number then a_1, a_2, $\ldots$, a_r are all even.

6. (a) Find the ternary (base 3) representation of 80.

(b) Find the base 10 representation of the integer whose ternary representation is $(12021)_3$.

7. By adapting Euclid's proof that there are infinitely many primes, show that there are infinitely many primes of the form $4m + 3$ with $m \in \mathbb{N}_0$. [*Hint:* show that any number of the form $4m + 3$ with $m \in \mathbb{N}_0$ is divisible by a prime also of this form.]

Bonus question: The game of Nim is important in combinatorial game theory. Find out the rules of Nim by searching on the web. Learn about the winning strategy which involves expressing the number of counters in each pile in binary.

MT181 Number Systems: Sheet 6

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 15th November.

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

2. Let A, B and C be mathematical statements. Show using truth tables that

(a) $A \implies B$ and $(\neg A) \vee B$ are logically equivalent;

(b) $\neg(A \vee B)$ and $(\neg A) \wedge (\neg B)$ are logically equivalent;

(c) $(A \vee B) \wedge C$ and $(A \wedge C) \vee (B \wedge C)$ are logically equivalently.

3. Let $z = re^{i\theta}$ be a complex number written in exponential form, so $r \in \mathbb{R}$, $r \geq 0$ and $\theta \in \mathbb{R}$.

(a) Prove that if $r = 2$ and $\theta = \pi/2 + 2n\pi$ for some $n \in \mathbb{Z}$ then $z = 2i$.

(b) Show conversely that if $z = 2i$ then $r = 2$ and $\theta = \pi/2 + 2n\pi$ for some $n \in \mathbb{Z}$.

[*Hint:* you should work from the definition of the exponential function given in Definition 2.1.]

(c) Write down a single statement, using the symbols $\exists$, $\wedge$, $\iff$, etc, that expresses the results proved in (a) and (b).

4. A statement is said to be a *tautology* if it is always true. For example, if P, Q and R are propositions then $P \vee (\neg P)$ is a tautology, because either P is true or $\neg P$ is true, but $P \implies Q$ is not a tautology, because it is false if P is true and Q is false. Which of the following are tautologies:

(i) $\big((P \implies Q) \wedge (Q \implies R)\big) \implies (P \implies R)$,

(ii) $\big(P \implies (Q \implies R)\big) \implies \big((P \implies Q) \implies R\big)$,

(iii) $\big((P \implies Q) \implies R\big) \implies \big(P \implies (Q \implies R)\big)$?

[*Hint:* You can use truth tables, or argue directly, as you prefer.]

5. (a) Let P be the proposition $(\forall x \in \mathbb{R})(x^2 > 0)$. Write $\neg P$ without using '$\neg$'. Is P true? Explain your answer.

(b) Let Q be the proposition $(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})(m \text{ divides } n)$. Write $\neg Q$ without using '$\neg$'. Is Q true? Explain your answer.

(c) Let R be the proposition $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(m \text{ divides } n)$. Write $\neg R$ without using '$\neg$'. Is R true? Explain your answer.

6. There are eight truth tables of the form below, where each of the starred entries is either true or false. For each such table, write down a proposition having that truth table using only parentheses and the symbols $A, B, \vee, \wedge$ and $\neg$.

A	B	
T	T	$\star$
T	F	$\star$
F	T	$\star$
F	F	F

Bonus question: There is an island whose population consists entirely of humans and vampires. The two species are indistinguishable to the eye, but humans always tell the truth and vampires always lie. To complicate matters, humans and vampires may be sane or insane. Sane inhabitants believe statements if and only if they are true, while insane inhabitants believe statements if and only if they are false.

Find a single question which you can ask an inhabitant of the island to determine whether they are a vampire.

[For many more questions like this see *What is the name of this book? The riddle of Dracula and other logical problems* by Raymond Smullyan (Prentice-Hall, 1978).

MT181 Number Systems: Sheet 7

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 22nd November.

1. Read Chapters 8 and 9 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009)

2. Let $X = \{1, 3, 5, 7\}$, $Y = \{2, 3, 6, 7\}$ and $Z = \{4, 5, 6, 7\}$. Draw a Venn diagram showing X, Y and Z. Express each of the sets $\{7\}$, $\{6, 7\}$, $\{3, 4, 5, 6, 7\}$, $\{3, 5, 6, 7\}$ in terms of X, Y and Z using only intersection $\cap$ and union $\cup$.

3. Let $n \in \mathbb{N}$ and let X and Y be the sets defined by

$$X = \{m \in \mathbb{N} : \gcd(m, n) = 2\}. \qquad Y = \{m \in \mathbb{N} : mn \text{ is a multiple of } 4\}$$

Prove that $X \subseteq Y$. [*Hint:* adapt the proof of Example 6.4(i).]

4. (a) Let X, Y be subsets of a set U. Prove that $(X \cap Y)' = X' \cup Y'$.

(b) Let X, Y and Z be sets. Prove that $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$.

(c) Let P, Q and R be propositions. Write down tautologies using P, Q, R and the logical symbols $\neg, \wedge, \vee, \iff$ that correspond to the results in (a) and (b).

5. Let the mapping $f : [2, \infty) \to \mathbb{R}$ be defined by $f(x) = x^2 - 4x - 1$.

(a) Show that f is injective.

(b) Show that f is not surjective.

Would your answers to (a) and (b) change if the domain of f was instead $[0, \infty)$?

6. Suppose that there is a 'universe set' U, whose elements are all sets. Russell's set R is defined to be the set of all sets that are not members of themselves. In symbols, $R = \{X \in U : X \notin X\}$.

(a) Give examples of sets Y and Z such that $Y \in R$ and $Z \notin R$.

(b) By considering first the possibility $R \in R$, then the possibility $R \notin R$, obtain a contradiction.

(This is Russell's paradox. It is avoided in modern axiomatic set theory by restricting the ways in which sets can be formed so that U and R are not sets.)

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 8

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 29th November.

1. Read Chapters 30 and 31 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009). The section of Chapter 30 on 'Types of infinity' is not part of this course, but it is on the syllabus for MT110.

2. Let $X = \{1, 2, 3\}$. Give an example of a function $f : X \to X$ that is neither injective nor surjective. Draw a diagram representing this function.

3. Let $f : \mathbb{R} \to \mathbb{R}$ be an injective function. Prove that the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = 5f(x)$ for all $x \in \mathbb{R}$ is injective.

4. Find an example of surjective functions $g : \mathbb{R} \to \mathbb{R}$ and $h : \mathbb{R} \to \mathbb{R}$ such that the function $g + h : \mathbb{R} \to \mathbb{R}$ defined by

$$(g + h)(x) = g(x) + h(x) \quad \text{for all } x \in \mathbb{R}$$

is not surjective.

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

(a) Show that if f and g are injective then $gf : X \to Z$ is injective.

(b) Show that if gf is injective then f is injective.

(c) Give an example where gf is injective but g is not injective.

(d) (Optional.) State and prove analogues of (b) and (c) for surjective functions.

6. For each of the relations $\sim$ below on a set X, decide whether it is (1) reflexive, (2) symmetric, (3) transitive. (Some relations might have more than one of these properties!) Give brief explanations or counterexamples as appropriate.

(a) X is the set of people taking MT181, $x \sim y$ if x and y were either both present or both absent at the MT181 lecture on Thursday 22nd November.

(b) X is the set of people taking MT181, $x \sim y$ if x and y were both present at the same MT181 lecture in the week this sheet was issued.

(c) X is the set of people in a lecture room, $x \sim y$ if x can see the eyes of y.

7. Let $X = \{1, 2, 3, 4, 5, 6, 7\}$. Define a relation $\equiv$ on X by

$$m \equiv n \iff m - n \in \{-6, -3, 0, 3, 6\}.$$

(a) Draw a diagram showing how elements of X are related by $\equiv$.

(b) Is $\equiv$ an equivalence relation?

8. Let $f : [0, \infty) \to [1, \infty)$ be defined by $f(x) = \sqrt{x+1}$ and let $g : [1, \infty) \to [0, \infty)$ be defined by $g(y) = (y-1)^2$.

(a) Find a formula for $f^{-1}(y)$ where $y \in [1, \infty)$.

(b) Find a formula for $g^{-1}(z)$ where $z \in [0, \infty)$.

(c) Show that $gf : [0, \infty) \to [0, \infty)$ is bijective. Using (a) and (b) find a formula for $(gf)^{-1}(z)$ where $z \in [0, \infty)$.

In (c) it will be helpful to use Theorem 7.9(iii) and the following remark.

Bonus question: Suppose that n points are put around the circumference of a circle and every pair of points is joined by a straight line through the circle. Let a_n be the greatest number of regions that the circle can be divided into. Calculate a_1, a_2, ..., a_6. Find and prove a general formula for a_n.

[*Hint:* once you have found a_1, a_2, ..., a_6, try typing them into Sloane's Online Encyclopedia of Integer Sequences, `www.oeis.org`.]

MT181 Number Systems: Sheet 9

Attempt all numbered questions. To be handed in during the MT181 lecture on Thursday 6th December.

1. Read Chapter 31 (if you have not already done so) and Chapter 32 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009).

2. Define a relation $\sim$ on the set of non-zero complex numbers by

$$z \sim w \iff \mathrm{Arg}(z) = \mathrm{Arg}(w).$$

(The principal argument Arg of a complex number was defined in Definition 1.10.)

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

(b) Find all $z \in \mathbb{C}$ such that $z \sim \mathrm{e}^{i\pi/4}$. Hence draw the equivalence class $[\mathrm{e}^{i\pi/4}]_\sim$ on an Argand diagram.

(c) Draw on the same diagram the equivalence class containing $2\mathrm{e}^{2i\pi/3}$.

3. (a) Find a relation on $\{1, 2, 3\}$ that is reflexive and symmetric but not transitive.

(b) Find a relation on $\{1, 2\}$ that is reflexive and transitive but not symmetric.

(c) Find a relation on a set of your choice that is symmetric and transitive but not reflexive.

(d) 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 $x \sim y \sim x$ and so by transitivity $x \sim x$. Thus $\sim$ is reflexive.'

Where is the flaw in this argument?

4. Recall that $\mathbb{Z} \times \mathbb{N}$ is the set of all ordered pairs (m, n) with $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. Define a relation $\equiv$ on $\mathbb{Z} \times \mathbb{N}$ by

$$(m, n) \equiv (m', n') \iff mn' = nm'.$$

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

(b) Write down three or more different elements $(m, n) \in \mathbb{Z} \times \mathbb{N}$ such that $(m, n) \equiv (3, 2)$. What do you notice about m/n in each case?

5. (a) Find an integer m such that $0 \leq m < 5$ and $m \equiv 2012 \bmod 5$.

(b) Find an integer m' such that $-5 \leq m' < 0$ and $m' \equiv 2012 \bmod 5$.

(c) Find an integer k such that $0 \leq k < 9$ and $k + 2 \equiv 88 \bmod 9$.

(d) Let $n \in \mathbb{N}$. Suppose that $a, b, x \in \mathbb{Z}$ are such that $a + x \equiv b + x \bmod n$. Show, from Definition 9.1, that $a \equiv b \bmod n$.

6. (a) The equivalence class $[3] \in \mathbb{Z}_5$ can be written as

$$[3] = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$$

Write down $[0], [1], [2] \in \mathbb{Z}_5$ in a similar way. Hence find an integer m such that $m \equiv 2 \bmod 5$ and $m \equiv 5 \bmod 6$.

(b) Find a solution $m \in \mathbb{Z}$ to the equation $5m \equiv 1 \bmod 13$.

7. Set a question on any part of the MT181 course.

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* (a) how useful you think solving your question would be to someone taking MT181, and (b) how hard you think your question is.

Your question should be in the style of previous questions on problem sheets, and could, if you wish, be obtained by making minor changes to any one of them.

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 A, B, 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.

Since good quality padlocks are quite expensive, the pirates were keen to arrive at this situation using as few padlocks as possible. How many padlocks are there on their treasure chest?

MT181 Number Systems: Sheet 10

Attempt all numbered questions. This sheet will not be marked. You can get help on it in workshops and office hours as usual.

The lecturer will be happy to answer questions over the vacation sent by email to `mark.wildon@rhul.ac.uk`.

1. Read Chapters 33, 34 and 35 of *How to think like a mathematician* by Kevin Houston (Cambridge University Press, 2009). Do at least one of the exercises in Exercises 33.1.

2. By Definition 9.1, $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. For example $[3] \in \mathbb{Z}_6$ is the congruence class of all integers m such that $m \equiv 3 \bmod 6$, so

$$[3] = \{\ldots, -9, -3, 3, 9, 15, \ldots\}.$$

(a) List the elements of $[0], [1], [2], [4], [5] \in \mathbb{Z}_6$ in a similar way.

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

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

(d) Does $[2]$ have an inverse (see Definition 9.10) in $\mathbb{Z}_6$?

3. Find the inverse of the element $[r]$ in $\mathbb{Z}_{37}$, where (i) $r = [14]$, (ii) $r = [10]$.

4. Let n be a composite number, so $n = ab$ for $a, b \in \mathbb{N}$ with $a, b \neq 1$.

(a) Show that $[a][b] = [0] \in \mathbb{Z}_n$.

(b) Deduce that $\mathbb{Z}_n$ is not a field if n is composite. (This is the converse to Theorem 9.11.)

[*Hint:* suppose for a contradiction that $[a]$ has an inverse $[r]$ such that $[r][a] = [1]$. Multiply both sides of the equation in (a) by $[r]$.]

5. The *Fibonacci numbers* are defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-2} + F_{n-1}$ for all $n \geq 2$. Let d_n be the final digit of F_n.

(a) Prove that $d_n \equiv F_n \bmod 10$.

(b) Prove that $d_n \equiv d_{n-2} + d_{n-1} \bmod 10$ for all $n \geq 2$.

(c) Does this sequence $d_0, d_1, d_2, \ldots$ repeat? If so, after how many terms? Could these answers have been predicted without doing any calculation?

6. Let $k, n, r \in \mathbb{N}$ and let

$$A = \{x \in \mathbb{N} : x \equiv r \bmod n\}$$
$$B = \{y \in \mathbb{N} : y \equiv r \bmod kn\}.$$

Show that $B \subseteq A$. Given an example to show that, in general, $B \neq A$.

7. Let n be a natural number. Suppose that $n = d_k d_{k-1} \dots d_1 d_0$ in base 10.

(a) Prove that $n \equiv d_0 + d_1 + \cdots + d_k \bmod 9$. [*Hint:* you need to show that the difference of the two sides is divisible by 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 $d_0 - d_1 + d_2 - \cdots + (-1)^k d_k$.

8. Let R be a ring.

(a) Prove Claim 9.12(ii), that the one element in R is unique. [*Hint:* adapt the proof of Claim 9.12(i).]

(b) Prove Claim 9.12(v), that if $x \in R$ then $-x = (-1)x = x(-1)$. [*Hint:* start by adding x to both sides.]

(c) Prove Claim 9.12(vi), that if $x \in R$ then $-(-x) = x$.

(d) Prove Claim 9.12(vii), that if $x, y \in R$ then $-(xy) = (-x)y = x(-y)$. Hence show that $(-x)(-y) = xy$.

9. (a) Multiply out the product $(x^2 + [1])(x^2 + [2]x + [2])(x^2 + x + [2])$ in $\mathbb{Z}_3[x]$.

(b) List the nine quadratic polynomials in $\mathbb{Z}_3[x]$ of the form $x^2 + ax + b$ where a, $b \in \mathbb{Z}_3$. How many roots does each polynomial have in $\mathbb{Z}_3$?

10. The finite field $\mathbb{F}_9$ is defined as follows. The elements of $\mathbb{F}_9$ are expressions of the form $a + bi$ where a, $b \in \mathbb{Z}_3$, and i is a special symbol with the property that $i^2 = [2]$. Addition and multiplication is defined just as for complex numbers.

(a) Show that $[2] = -[1]$ in $\mathbb{Z}_3$ and so $i^2 = -[1]$.

(b) Write out the addition and multiplication tables for $\mathbb{F}_9$.

(c) Show that every non-zero element of $\mathbb{F}_9$ has an inverse.

Note that in $\mathbb{Z}_9$ we have $[3][3] = [9] = [0]$. So, by Question 4, $[3]$ has no inverse in $\mathbb{Z}_9$. This shows that $\mathbb{Z}_9$ and $\mathbb{F}_9$ are different number systems.

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.]