

# MAS114 revision notes

James Cranch

You *should* know everything in these notes, to do the Semester 1 questions in the MAS114 exam. However, these notes are *not* intended to be a complete list of everything you should know; merely a revision aid.

## Sets

A *set* is a collection of objects. The objects in a set are often called its *elements*.

We write  $a \in S$  to mean “ $a$  is in  $S$ ”, and  $a \notin S$  to mean “ $a$  is not in  $S$ ”.

We also write  $|S|$  to denote the *size* of  $S$ : the number of elements in it.

Two sets  $A$  and  $B$  are equal if they have the same members.

If  $A$  and  $B$  are sets, we write  $A \subset B$  to mean “if  $x$  is a member of  $A$  then  $x$  is also a member of  $B$ ”. We say that  $A$  is a *subset* of  $B$ , or that  $A$  is *contained* in  $B$ .

The empty set, which could be written  $\{\}$ , is more commonly written  $\emptyset$ .

## Russell’s paradox

Consider the set  $S$  of all sets which are not elements of themselves:

$$S = \{A \mid A \notin A\}.$$

This set is self-contradictory.

We can ask:  $S$  a member of itself? If  $S \in S$ , then by the definition of  $S$ , we have  $S \notin S$ . On the other hand, if  $S \notin S$ , then again by the definition of  $S$  we have  $S \in S$ .

## Functions

Given sets  $A$  and  $B$ , a *function* (sometimes called a *map*)  $f : A \rightarrow B$  gives for each element  $a \in A$  a unique element  $f(a) \in B$ . The set  $A$  is called the *domain* of  $f$ , and  $B$  is called the *codomain* of  $f$ . We call  $f(a)$  the *value* of  $f$  at  $a$ , or the *image* of  $a$  under  $f$ .

## Equality of functions

Two functions are equal if:

- they have the same domain and codomain, as  $f, g : A \rightarrow B$ ; and
- their values are equal, for every point in the domain: in other words, for all  $a \in A$ , we have  $f(a) = g(a)$ .

## Composition

Given two functions  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , we can define their *composite*  $g \circ f : A \rightarrow C$  by the rule:

$$g \circ f(x) = g(f(x)).$$

## Injective, surjective, bijective

- A function  $f : A \rightarrow B$  is said to be *injective* if, for any two elements  $a_1, a_2 \in A$  with  $a_1 \neq a_2$ , then  $f(a_1) \neq f(a_2)$ . I think of this as saying that “nothing is hit twice”, or equivalently that “no two elements of the domain have the same image”.
- A function  $f : A \rightarrow B$  is said to be *surjective* if, for every element  $b \in B$ , there is some element  $a \in A$  with  $f(a) = b$ . I think of this as saying that “every element of the codomain is hit at least once”.
- A function  $f : A \rightarrow B$  is said to be *bijective* if it is both injective and surjective. I think of this as saying that “every element of the codomain is hit exactly once”.

## Logical operators

Let  $A$  and  $B$  be statements.

We say that  $A$  *implies*  $B$ , written  $A \Rightarrow B$ , to mean “if  $A$  is true, then  $B$  also has to be true”. The *contrapositive* of this statement is the statement  $(\neg B) \Rightarrow (\neg A)$ .

The *negation* of  $A$ , written  $\neg A$  and often pronounced “not  $P$ ”, is the statement “ $A$  is false”.

We write  $A \Leftrightarrow B$ , pronounced “ $A$  is equivalent to  $B$ ” for the statement that  $A$  is true if and only if  $B$  is true.

The statement  $A \wedge B$ , pronounced “ $A$  and  $B$ ”, is the statement that both  $A$  and  $B$  is true.

The statement  $A \vee B$ , pronounced “ $A$  or  $B$ ”, is the statement that at least one of  $A$  or  $B$  (and possibly both) is true.

## Quantifiers

The symbol  $\forall$  means *for all*, and the symbol  $\exists$  means *there exists*.

## Negating quantifiers

$\neg(\forall x \in X, P(x))$  is equivalent to  $\exists x \in X$  s.t.  $\neg P(x)$ .  
 $\neg(\exists x \in X$  s.t.  $P(x))$  is equivalent to  $\forall x \in X, \neg P(x)$ .

## Induction

Let  $P(n)$  be a statement that depends on a natural number  $n$ . Then, if

- (i) the statement  $P(0)$  is true, and
- (ii) for all  $k \in \mathbb{N}$ , if  $P(k)$  is true, then  $P(k + 1)$  is true,

then the statement  $P(n)$  is true for all  $n \in \mathbb{N}$ .

### Strong induction

Let  $P(n)$  be a statement that depends on a natural number  $n$ . Then if

- (i)  $P(0)$  is true, and
- (ii) for all  $k$ , if  $P(0), P(1), \dots, P(k)$  are all true, then  $P(k + 1)$  is also true,

then  $P(n)$  is true for all  $n \in \mathbb{N}$ .

### The well-ordering principle

The *well-ordering principle* for  $\mathbb{N}$  says that any nonempty subset of  $\mathbb{N}$  has a least element.

The well-ordering principle for  $\mathbb{N}$  and the principle of strong induction are equivalent.

### Divisors, multiples, etc

Let  $a$  and  $b$  be integers. We say that  $a$  *divides*  $b$  if there exists an integer  $n$  such that  $an = b$ .

We also might say that  $b$  is a *multiple* of  $a$ , or that  $a$  is a *divisor* of  $b$ , or that  $a$  is a *factor* of  $b$ , or that  $a$  *goes into*  $b$ .

### Prime and composite numbers

An integer  $p > 1$  is said to be *prime* if it has no positive factors except for 1 and  $p$  itself.

An integer  $n > 1$  is said to be *composite* if it is not prime: that is, if it does have positive factors other than 1 and  $n$ .

### Euclid's theorem

There are infinitely many prime numbers.

### The gcd and the lcm

The *greatest common divisor* of  $a$  and  $b$ , written  $\gcd(a, b)$ , is the largest positive integer which is a divisor both of  $a$  and  $b$ .

Given two integers  $a$  and  $b$ , the *least common multiple*  $\text{lcm}(a, b)$  is the smallest positive integer which is a multiple both of  $a$  and  $b$ .

Two integers  $a$  and  $b$  are said to be *coprime*, or *relatively prime*, if  $\gcd(a, b) = 1$ .

### Properties of the gcd

For all integers  $a, b$  and  $k$ , we have

$$\gcd(a, b) = \gcd(b, a),$$

$$\gcd(a, 0) = \gcd(a, a) = a,$$

$$\gcd(a, 1) = 1,$$

$$\gcd(a, b) = \gcd(a, -b),$$

$$\gcd(a, b) = \gcd(a + kb, b).$$

### Division with remainder

Let  $a$  and  $b$  be integers, with  $b > 0$ . One can write

$$a = qb + r$$

for integers  $q$  (the *quotient*) and  $r$  (the *remainder*) such that  $0 \leq r < b$ .

### Euclid's algorithm

Suppose we must calculate the greatest common divisor of two integers: call them  $a_0$  and  $a_1$  with  $0 < a_1 < a_0$ . (If they're not positive, or not in the right order, we can change their signs or swap them over, to sort this out.)

By division with remainder, we can write  $a_0 = q_1 a_1 + a_2$  for some integers  $q_1$  and  $a_2$  with  $0 \leq a_2 < a_1$ . But then we have

$$\gcd(a_0, a_1) = \gcd(a_2 + q_1 a_1, a_1) = \gcd(a_2, a_1) = \gcd(a_1, a_2).$$

Since  $a_2 < a_1 < a_0$ , we've made both numbers smaller by doing this. If  $a_2 > 0$ , we continue, writing  $a_1 = q_2 a_2 + a_3$  for some integers  $q_2$  and  $a_3$  with  $0 \leq a_3 < a_2$ , and get

$$\gcd(a_1, a_2) = \gcd(a_3 + q_2 a_2, a_2) = \gcd(a_3, a_2) = \gcd(a_2, a_3).$$

We keep going like this, defining  $a_3, a_4$ , and so on (and  $q_3, q_4$ , and so on too). These get smaller and smaller, but are nonnegative, so eventually we get  $a_k = 0$  for some  $k$ .

### Bezout's Lemma

Let  $a$  and  $b$  be two integers with  $\gcd(a, b) = d$ . Then there are integers  $m$  and  $n$  such that  $ma + nb = d$ .

In fact, for any integer  $e$ , we can write  $e$  in the form  $e = ma + nb$  if and only if  $d \mid e$ .

### Primes and factors

Let  $p$  be a prime, and  $a$  and  $b$  be integers. Then, if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .

Moreover, let  $a_1, \dots, a_n$  be integers. Then if  $p \mid a_1 \cdots a_n$ , then  $p \mid a_i$  for some  $i$ .

### The fundamental theorem of arithmetic

Any positive integer  $n$  can be written as a product of primes in exactly one way, up to reordering.

### Congruences: definition

We say that  $a$  is congruent to  $b$  modulo  $m$  if  $m \mid (a - b)$ . Often we abbreviate, and say congruent *mod*  $m$ .

We use the notation

$$a \equiv b \pmod{m}$$

to indicate that  $a$  and  $b$  are congruent modulo  $m$ .

### Properties of congruences

- (a) We always have  $a \equiv a \pmod{m}$ ;
- (b) If  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ ;
- (c) If  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ , then  $a \equiv c \pmod{m}$ ;
- (d) If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$ ;
- (e) If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$ ;
- (f) If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$ .

### Reducing mod $b$

Let  $a$  and  $b$  be integers, with  $b > 0$ . Then  $a$  is congruent (modulo  $b$ ) to a unique integer in the set

$$\{0, 1, \dots, b - 1\}.$$

### When are residues invertible?

Let  $a$  and  $m$  be integers. There is an integer  $b$  such that  $ab \equiv 1 \pmod{m}$  if and only if  $\gcd(a, m) = 1$ .

When such a  $b$  does exist, it's unique (modulo  $m$ ).

### Multiplying and inverting invertibles

If  $a$  is invertible modulo  $m$ , then so is  $a^{-1}$ , with inverse given by  $(a^{-1})^{-1} \equiv a \pmod{m}$ .

If  $a$  and  $b$  are both invertible, then  $ab$  is too, with inverse given by

$$(ab)^{-1} \equiv a^{-1}b^{-1} \pmod{m}.$$

### The Chinese remainder theorem

Let  $m_1$  and  $m_2$  be coprime, and let  $a_1$  and  $a_2$  be any integers. The simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

have a solution modulo  $m_1m_2$ .

### Finite multiplicative orders

Let  $a$  and  $m$  be coprime integers. Then there is some positive  $n$  such that

$$a^n \equiv 1 \pmod{m}.$$

### Fermat's little theorem

Let  $p$  be prime, and let  $a$  be an integer coprime to  $p$ . Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

### Euler's function $\varphi$

*Euler's function* (sometimes called the *totient function*)  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  is defined by taking  $\varphi(n)$  to be the number of integers between 1 and  $n$  (inclusive) which are coprime to  $n$ .



### The Fermat-Euler theorem

Let  $a$  and  $n$  be integers with  $\gcd(a, n) = 1$ . Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

### Square roots of 1 modulo a prime

Let  $p$  be a prime, and let  $a$  be an integer with the property that  $a^2 \equiv 1 \pmod{p}$ . Then either  $a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$ .

### Wilson's theorem

We have  $(n - 1)! \equiv -1 \pmod{n}$  if and only if  $n$  is prime.

### $\sqrt{2}$ is irrational

There is no rational number  $x \in \mathbb{Q}$  such that  $x^2 = 2$ .

### Rational and irrational numbers

Let  $x$  be irrational, and  $y$  be rational. Then  $x + y$  is irrational. Also, if  $y$  is nonzero, then  $xy$  is irrational.

### Convergence: definition

Let  $x$  be a real number. A sequence of real numbers  $a_0, a_1, a_2, \dots$  is said to *converge to  $x$*  if we have

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} \quad \text{s.t.} \quad \forall n > N, \quad |a_n - x| < \epsilon.$$

We say that a sequence  $(a_i)_{i \in \mathbb{N}} = a_0, a_1, \dots$  is *convergent* if it converges to some  $x$ .

### Limits are unique

A sequence  $a_0, a_1, \dots$  cannot converge to two different real numbers  $x$  and  $y$ .

### Inequalities between limits

Suppose that  $a_0, a_1, \dots$  and  $b_0, b_1, \dots$  are sequences, and suppose the sequence  $(a_i)_{i \in \mathbb{N}}$  converges to  $a$ , and the sequence  $(b_i)_{i \in \mathbb{N}}$  converges to  $b$ .

If  $a_i \leq b_i$  for all  $i$ , then  $a \leq b$ .

### The sandwich lemma

Suppose we have three sequences:  $a_0, a_1, a_2, \dots$ , and  $b_0, b_1, b_2, \dots$  and  $c_0, c_1, c_2, \dots$ , such that:

- (i) the sequences  $(a_i)_{i \in \mathbb{N}}$  and  $(c_i)_{i \in \mathbb{N}}$  both converge to the same number  $x$ ; and
- (ii) for all  $i$  we have

$$a_i \leq b_i \leq c_i$$

Then the sequence  $(b_i)_{i \in \mathbb{N}}$  also converges to  $x$ .

### Adding convergent sequences

Let  $a_0, a_1, \dots$  be a sequence that converges to  $x$ , and let  $b_0, b_1, \dots$  be a sequence that converges to  $y$ . Then the sequence

$$a_0 + b_0, \quad a_1 + b_1, \quad \dots$$

converges to  $x + y$ .

### Cauchy sequences: definition

A sequence  $a_0, a_1, a_2, \dots$  is said to be *Cauchy* if

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} \quad \text{s.t.} \quad \forall m, n > N, \quad |a_m - a_n| < \epsilon.$$

That is, a sequence is Cauchy if whatever  $\epsilon$  you choose, there is some point  $N$  beyond which all terms of the sequence  $a_m, a_n$  are within  $\epsilon$  of each other.

### Convergent versus Cauchy

Any convergent sequence is a Cauchy sequence.