# SMA205 - Introduction to algebra

Welcome to the course SMA205 - Introduction to Algebra.

- Summaries of all lectures will be distributed, with page numbers so that you will know if you are missing some page.
- The exam will most probably be given in December. There will be more information on the exam later.
- With the summaries there will also be exercises and problems. The exercises will be easy, and will serve only as a help for you to check that everything is clear. The problems will be harder and will require some thought. The student who attempts all problems will be well prepared for the exam.
- You are encouraged to ask questions whenever something is unclear. You can ask during the lectures, after the lectures, in my office, or by email.

The outline of the course is as follows:

- Review of sets, relations and functions
- Elementary number theory
- Applications to cryptography
- Introduction to abstract algebra

There will soon be a course web page:

`www.andreasholmstrom.org/teaching/sma205/sma205.html`

Here you will find copys of the lecture notes and additional online references for further reading. Nothing of this is necessary for the exam, but for those who want to learn more, it is a good starting point.

You can always email me at `andreas.holmstrom@gmail.com` if you have any questions.

# 1 Review of sets, relations and functions

You will already be familiar with the notions of set, relation and function, but since these are absolutely fundamental to everything that follows, we will quickly review them.

## 1.1 Sets

We can think of a *set* as any collection of objects. Most often these objects will be numbers. The objects that belong to a set are called *members* or *elements* of the set. A set can be either *finite* or *infinite*. We will use capital letters, mainly A, B, C, S, T, to denote sets, and small letters (a, b, c, ...) for the elements of a set. We use the notation

$$a \in S$$

to say that $a$ is a member of the set $S$. We also write $a \notin S$ if $a$ is not a member of $S$. If $S$ and $T$ are two sets, and every element of $S$ is also an element of $T$, then we say that $S$ is a *subset* of $T$, and we write

$$S \subseteq T$$

### 1.1.1 How to describe a set

There are (at least) two ways to describe a set. In both cases, we uses braces $\{\ldots\}$ to show that we are dealing with a set. The first way is to *list* the elements of the set. For example, if the set $S$ has three elements, namely the numbers 1, 3, and 7, we may write

$$S = \{1, 3, 7\}$$

to describe the set $S$. It does not matter in which order we list the elements. Thus $\{2, 3\}$ is the same set as $\{3, 2\}$. Also, repeated elements make no difference, so $\{b, a\}$ is the same set as $\{a, b, a\}$.
If the set is infinite, we use dots to indicate that the sequence continues. For example, the set of natural numbers can be described as

$$\{0, 1, 2, 3, \ldots\}.$$

The set of natural numbers will be denoted by $\mathbb{N}$.
The second way to describe a set $S$ is to specify a particular property that characterizes the elements of the set. For integers, such a property might for example be "to be even" or "to be greater than 5" or "to be a prime number". However, it is not enough to specify a property. To illustrate this, consider "the set of all numbers greater than 2 and smaller than 10". Which numbers are in this set? Is 5 in the set? You would probably say yes. Is

$\pi$ in the set? Well, that depends on what you mean by "numbers". The point here is that you must first specify a basic set of allowed objects, and then give a property that defines your set from these allowed objects. To describe the set of all natural numbers between 2 and 10 we write

$$\{x \in \mathbb{N} \mid x > 2 \text{ and } x < 10\}$$

We read this as "the set of all $x$ in $\mathbb{N}$ such that $x$ is greater than 2 and smaller than 10. Of course, $\pi$ is not a member of this set. In general, to describe the set of all objects in $S$ that satisfies property $P$, we write

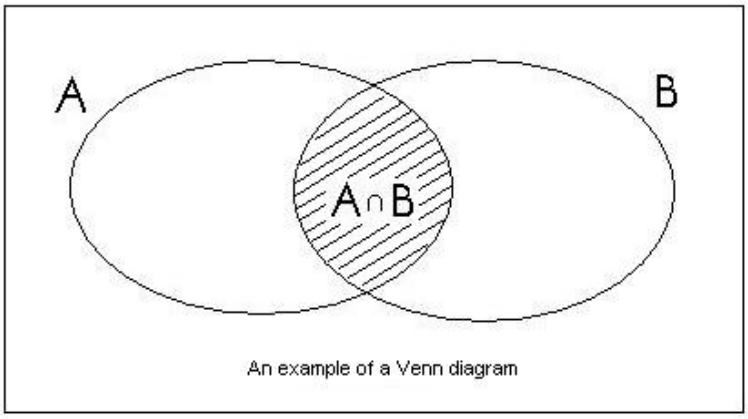
$$\{x \in S \mid x \text{ satisfies the property P}\}$$

This way of describing a set is generally more useful than the first, and will be used in most cases in this course.
There is actually a third way to describe a set: to simply describe it in words. For example "the set of all natural numbers that are a multiple of five", of "the set of all people in the world who have the letter h in their surname".

### 1.1.2 Constructions on sets

Given two sets $A$ and $B$, we can define the following sets:

- $A \cup B$, the *union* of $A$ and $B$: the set of all elements that are in $A$ *or* in $B$, or in both.
- $A \cap B$, the *intersection* of $A$ and $B$: the set of all elements that are both in $A$ and $B$.
- $A \setminus B$, the set of all elements that are in $A$ but not in $B$.



An example of a Venn diagram

All of these can be illustrated by Venn diagrams, as explained in the lecture. We say that two sets $A$ and $B$ are *equal*, and write $A = B$, if they contain exactly the same elements. We say that they are *disjoint*, if they have no elements in common. There is exactly one set which has no elements at all. It is called the *empty set*, and is denoted by the symbol $\emptyset$. It is a subset of every set.

### 1.1.3 Cartesian product

If $A$ and $B$ are two sets, we want to consider pairs $(a, b)$, where the first element $a$ belongs to $A$ and the second element $b$ belongs to $B$. The set of all such pairs is called the *Cartesian product* of $A$ and $B$, and is denoted by $A \times B$. Let us take some examples:

- Let $A = \{1, 2\}$ and let $B = \{x, y\}$. Then $A \times B = \{(1, x), (2, x), (1, y), (2, y)\}$.
- Let $A = B = \mathbb{R}$, the real line. Then $A \times B$ is the plane.
- Let $A = \{5\}$ and let $B = \{u, v, z\}$. Then $A \times B = \{(5, u), (5, v), (5, z)\}$.

Now let $A = \{x, y\}$. What are the elements of $A \times A$? Well, $A \times A$ is the set $\{(x, x), (x, y), (y, x), (y, y)\}$. The point here is that $(x, y)$ is not the same element as $(y, x)$. We express this by saying that the elements of the Cartesian product are *ordered pairs*. For two ordered pairs to be equal, their first entries must be equal and their second entries must be equal.

### 1.1.4 Exercises

For exercises E1 to E18, let

$$\begin{aligned} A &= \{x \in \mathbb{N} \mid 1 \leq x \leq 6\} \\ B &= \{2, 4, 6\} \\ C &= \{6, 7\} \end{aligned}$$

Decide whether the following statements are true or false:
**E1** $B$ and $C$ are disjoint.
**E2** $2 \in A$.
**E3** $2 \notin B$.
**E4** $A \cap C = B \cap C$.
**E5** $A \subseteq B$.
**E6** $C \subseteq B$.
**E7** $B \subseteq A$.
Describe the following sets:
**E8** $A \setminus B$.
**E9** $B \cap C$
**E10** $A \cup B$

**E11** $B \times C$
**E12** $B \cup (A \cap C)$
**E13** $C \cap (A \cup B)$
**E14** $B \setminus A$
**E15** $B \cup \emptyset$
**E16** $A \cap \emptyset$
**E17** How many elements are there in $A \times C$?
**E18** How many elements are there in $A \times (B \cap C)$?
In exercises E19 to E25, let $A$, $B$ and $C$ be any sets.
**E19** Is $A$ a subset of $A$?
**E20** Is $\emptyset$ a subset of $A$?
**E21** Is $A$ a subset of $A \times A$?
**E22** Is $\emptyset$ a subset of $A \times A$?
**E23** Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(There are two ways of doing this. One way is to draw the Venn diagram of both sides and check that they are equal. The other way is to show that any element of the left hand side must be in the right hand side, and the other way around.)
**E24** Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
**E25** Prove that $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
Determine the number of elements in the following sets:
**E26** $\{x \in \mathbb{N} \mid x = x^2\}$.
**E27** $\{a \in \mathbb{N} \mid a < 19 \text{ and } a = 2^k \text{ for some } k \in \mathbb{Z}\}$.
**E28** $\{x \in \mathbb{N} \mid x \text{ is even and } x \leq 23\}$.
Answer the following questions:
**E29** If set $A$ has 2 elements, how many elements does $A \times A$ have?
**E30** If the finite set $A$ has $n$ elements, how many elements does $A \times A$ have?
**E31** If the set $A$ has 1 elements, how many subsets does $A$ have?
**E32** If the set $A$ has 2 elements, how many subsets does $A$ have?

## 1.2 Relations

If we are given a set $S$, we shall be interested in relations between the elements of the set. Let us consider the set of integers, to see some examples. The following are relations on the set of integers:

- "$a$ is less than or equal to $b$"
- "$a$ divides $b$" (this will be defined later)
- "$a$ is equal to $b$"
- "$a$ has the same sign[1] as $b$"

[1]Here we consider negative numbers to have a minus sign, positive numbers to have a plus sign, and the number 0 to have a neutral sign

When we are given a relation we can consider the set of all ordered pairs that satisfy the relation. Take for example the first relation in the above list. This defines a set $R$, in which for example $(4, 14)$ and $(5, 5)$ are members, while $(5, 4)$ and $(14, 4)$ are not. Similarly, consider the set $S$ of all pairs satisfying the last relation in the list. In this case $(-2, -3)$ and $(5, 99)$, and $(0, 0)$ are all in the set $S$, while $(1, -1)$ and $(0, 1)$ are not in $S$. We can go on like this, and observe that every relation on a set $A$ determines a certain subset of $A \times A$. In fact, this point of view is used as the abstract definition of a relation:

**Definition 1.** A *relation* on a set $A$ is a subset of $A \times A$.

If $R$ is any relation on a set, we write $a\ R\ b$ if the pair $(a, b)$ belongs to the relation. The following definitions will allow us to gain a better understanding of relations.

**Definition 2.** A relation is *symmetric* if $a\ R\ b$ implies $b\ R\ a$.
A relation is *reflexive* if $a\ R\ a$ for every $a$.
A relation is *transitive* if $a\ R\ b$ and $b\ R\ c$ implies $a\ R\ c$.

Examples: the relation $\leq$ is reflexive and transitive, but not symmetric. The relation $=$ is symmetric, reflexive, and transitive.

### 1.2.1 Equivalence relations

We define a *partition* of a set $S$ to be a collection of nonempty pairwise disjoint subsets of $S$ set whose union is $S$. Each subset in a partition is called a *cell*. If we are given a partition of a set $S$, we can consider the following relation: "$a$ and $b$ are in the same cell". Thus every partition determines a relation. If $a$ is an element, we write $cl(a)$ for the cell that contains $a$.

**Definition 3.** An *equivalence relation* is a relation determined by a partition, by the rule "$a$ and $b$ are in the same cell".

For example, consider the partition of the integers into the three sets of negative numbers, positive numbers, and the set $\{0\}$. The relation determined by this partition is the last relation in the above list of examples.

**Theorem 1.** A relation is an equivalence relation if and only if it is symmetric, reflexive and transitive.

*Proof.* Given in lectures. □

### 1.2.2 Exercises

For exercises E33 to E40, let $R$ be the relation $>$ on the natural numbers. Are the following statements true or false?
**E33** $(5, 4) \in R$
**E34** $R$ is symmetric.
**E35** $(9, 9) \notin R$.
**E36** $R$ is transitive.
**E37** $8\ R\ 1$.
**E38** $R$ is reflexive.
**E39** $(2, -1) \in R$.
**E40** $R$ is an equivalence relation.
For exercises E41 to E48, define a relation $R$ on $\mathbb{N}$ by

$$a\ R\ b \quad \text{if} \quad (a - b) \text{ is an even integer}$$

Are the following statements true or false?
**E41** $(5, 9) \in R$
**E42** $R$ is reflexive.
**E43** $(10, 1) \notin R$.
**E44** $R$ is symmetric.
**E45** $7\ R\ 4$.
**E46** $R$ is transitive.
**E47** $(2, 2) \in R$.
**E48** $R$ is an equivalence relation.
For exercises E49 to E55, let $A = \{1, 2, 3, \ldots, 9, 10\}$. Are the following lists of sets partitions of $A$?
**E49** $\{1, 2\},\ \{3, 5, 7, 9\},\ \{4, 6, 8\}$.
**E50** $\{a \in A \mid a \text{ is even}\},\ \{a \in A \mid a \text{ is odd}\}$.
**E51** $\{1, 2\},\ \{3, 5, 7\},\ \{2, 4, 6, 7, 8, 9, 10\}$.
**E52** $\{8, 4, 2\},\ \{9, 1, 10\},\ \{5\},\ \{7, 3, 6\}$.
**E53** $\{1, 3, 5, 7\},\ \{0, 2, 4, 6, 8\},\ \{11, 10, 9\}$.
**E54** What is the maximal possible number of cells in a partition of $A$?
**E55** What is the minimal possible number of cells in a partition of $A$?

## 1.3 Functions

Let $A$ and $B$ be sets. A function $f$ from $A$ to $B$ can be thought of as some kind of rule, or machine, that assigns one element of $B$ to each element of $A$. For example, if $A = B = \mathbb{N}$, there is a function which to each element $n \in \mathbb{N}$ assigns the square $n^2 \in \mathbb{N}$. A function is sometimes called a *map* or *mapping*. If an element $b \in B$ is assigned to $a \in A$ we say that $a$ is *sent to* $b$, or that $a$ *maps to* $b$, and we write $f(a) = b$.
Now let $f$ be a function from $A$ to $B$. We can then consider the set of all pairs $(a, b) \in A \times B$ such that $f(a) = b$. This is a subset of $A \times B$, called the

*graph* of $f$. The graph of a function has the following property: for every $a \in A$ there is a unique element $b \in B$ such that $(a, b)$ is in the graph. This leads to the abstract definition of a function:

**Definition 4.** A *function* from a set $A$ to a set $B$ is a subset $f$ of $A \times B$ such that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$. Usually we write $f(a) = b$ instead of $(a, b) \in f$.

If $f$ is a function from $A$ to $B$ we write $f : A \to B$. We call $A$ the *domain* of $f$ and $B$ the *codomain* of $f$. The set

$$im(f) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}$$

is called the *image* of $f$. If an element $a$ is mapped to an element $b$ we write $a \mapsto b$. The most common way of specifying a function is illustrated by the following example, in which we take $A = B = \mathbb{N}$.

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto x^2 \end{aligned}$$

This function, which sends each natural number to its square, can also be described by the formula

$$f(x) = x^2$$

which is perhaps more familiar.

**Definition 5.** Let $f : A \to B$ be a function. We say that $f$ is *injective* (or *one-to-one*) if $f(x) = f(y)$ implies $x = y$. We say that $f$ is *surjective* (or *onto*) if for every $b \in B$, there is some $a \in A$ such that $f(a) = b$. We say that $f$ is *bijective* if it is both surjective and injective.

In other words, $f$ is surjective if $im(f)$ equals $B$, and $f$ is injective if two different elements of $A$ always are mapped to two different elements of $B$ (hence "two-to-two" would actually be a better word than "one-to-one"). If $f : A \to B$ and $g : B \to C$ are functions, we can define a function $h$ from $A$ to $C$ by the rule $h(a) = g(f(a))$. This function called the *composite* and is denoted by $g \circ f$.

### 1.3.1 Exercises

For exercises E56 to E70, define

$$\begin{aligned} g : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto x^2 - x + 1 \end{aligned}$$

and let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = x + 2$.
**E56** Is $f$ injective?

**E57** Is $f$ surjective?
**E58** Is $f$ bijective?
**E59** What is the domain of $f$?
**E60** What is the codomain of $f$?
**E61** What is the image of $f$?
**E62** Is $g$ injective?
**E63** Is $g$ surjective?
**E64** Is $g$ bijective?
**E65** What is the codomain of $g$?
**E66** Write down some elements of $im(g)$.
**E67** Compute $g \circ f(7)$.
**E68** Compute $f \circ g(7)$.
**E69** Is $f \circ g$ injective?
**E70** Is $g \circ f$ injective?

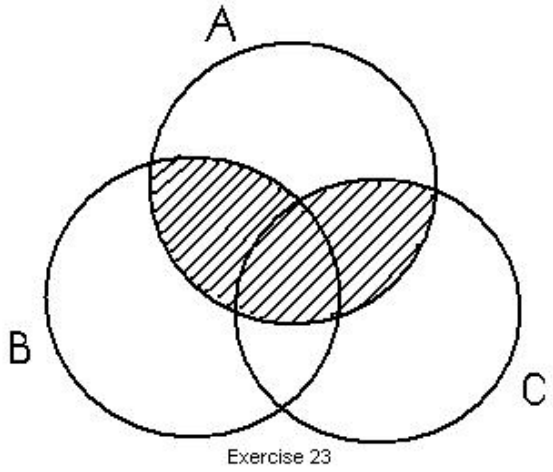
## 1.4 Problems

**P1** If $A$ has five elements and $B$ has three elements, how many different functions are there from $A$ to $B$?
**P2** Try to find a relation on some set which is reflexive and symmetric, but not transitive.
**P3** If the set $A$ has $n$ elements, how many subsets does $A$ have?
**P4** Is it true that the composite of two injective functions is injective?
**P5** Is it true that the composite of two surjective functions is surjective?
**P6** Define a function $f : \mathbb{N} \to \mathbb{N}$ by $f(a) =$ "sum of the digits of $a$". This means that for example $f(2) = 2$, $f(35) = 8$ and $f(18247) = 22$. Let $g = f \circ f$. Answer the following questions:
(i) Compute $f(669)$.
(ii) Is $f$ injective?
(iii) Is $f$ surjective?
(iv) Is $f$ bijective?
(v) Compute $g(15005)$.
(vi) Compute $g(259781)$.
(vii) What is the codomain of $g$?
(viii) What is the domain of $g$?
(ix) Is $g$ injective?
(x) Is $g$ surjective?

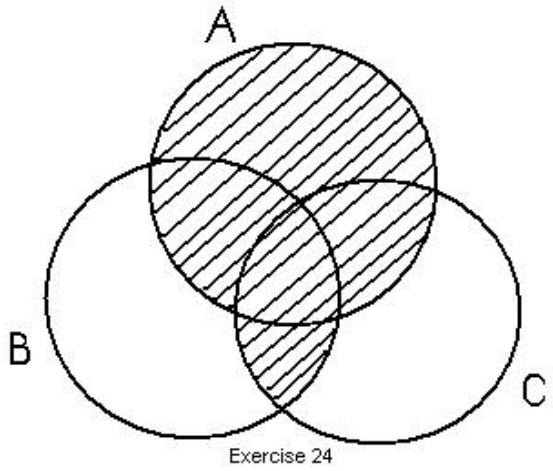
## 1.5 Answers and solutions

### 1.5.1 Exercises E1 to E70

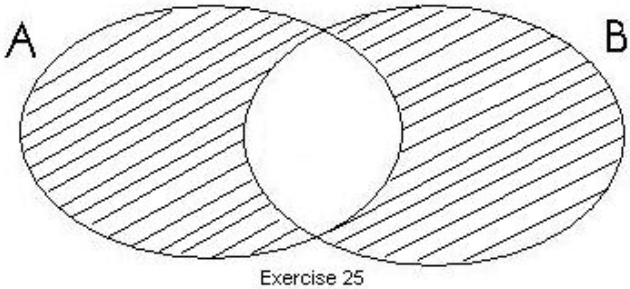
**E1** False. **E2** True. **E3** False. **E4** True. **E5** False. **E6** False. **E7** True. **E8** $\{1, 3, 5\}$. **E9** $\{6\}$. **E10** $\{1, 2, 3, 4, 5, 6\}$. **E11** $\{(2, 6), (2, 7), (4, 6), (4, 7), (6, 6), (6, 7)\}$. **E12** $\{2, 4, 6\}$. **E13** $\{6\}$. **E14** $\emptyset$. **E15** $\{2, 4, 6\}$. **E16** $\emptyset$. **E17** 12 elements. **E18** 6 elements. **E19** Yes. **E20** Yes. **E21** No. **E22** Yes. **E23, E24, E25** In each exercise, draw the Venn diagrams of both sets, and check that they are equal. See the pictures. **E26** 2 elements. **E27** 5 elements.



Exercise 23



Exercise 24



Exercise 25

**E28** 12 elements. **E29** 4 elements. **E30** $n^2$ elements. **E31** 2 subsets. **E32** 4 subsets. **E33** True. **E34** False. **E35** True. **36** True. **E37** True. **E38** False. **E39** False (because $-1 \notin \mathbb{N}$). **E40** False. **E41** True. **E42** True. **E43** True. **E44** True. **E45** False. **46** True. **E47** True. **E48** True. **E49** No. **E50** Yes. **E51** No. **E52** Yes. **E53** No. **E54** 10 cells. **E55** 1 cell. **E56** Yes. **E57** No. **E58** No. **E59** $\mathbb{N}$. **E60** $\mathbb{N}$. **E61** $\{x \in \mathbb{N} \mid x \geq 2\}$. **E62** No (because $f(0) = f(1)$). **E63** No (because 2 is not in the image). **E64** No. **E65** $\mathbb{N}$. **E66** 1, 3, 7, 13 (for example). **E67** 73. **E68** 45. **E69** No (because $f(0) = f(1)$. **E70** Yes.

### 1.5.2 Problems P1 to P6

The problems were discussed in the tutorial class. Here we just give brief answers and some hints.
**P1** Answer: 243 different functions. In general, if $A$ has $m$ elements and $B$ has $n$ elements, then there are $n^m$ different functions from $A$ to $B$.
**P2** One example is the following relation on the set of integers:

$$a \; R \; b \quad \text{if} \quad |a - b| \leq 1$$

Verify that this relation is reflexive and symmetric, but not transitive.
**P3** Try to first answer the question for $n = 1$, $n = 2$, $n = 3$. Try to guess a pattern. Then try to prove your guess.
**P4** Yes.
**P5** Yes.
**P6** Answers: (i) 21. (ii) No. For example, $f(10) = f(1)$. (iii) Yes. If $n \in \mathbb{N}$ is any given number, we can consider the number

$$a = \underbrace{111\ldots1}_{n \text{ times}}$$

Clearly, we have $f(a) = n$.
(iv) No. (v) 2. (vi) 5. (vii) $\mathbb{N}$. (viii) $\mathbb{N}$. (ix) No. (x) Yes, see problem 5 above.

# 2 Elementary number theory

## 2.1 Introduction

Elementary number theory is concerned with properties of the integers. Hence we shall be interested in the following sets:

- The set if integers $\{\ldots -2, -1, 0, 1, 2, 3, \ldots\}$, denoted by $\mathbb{Z}$
- The set of natural numbers $\{0, 1, 2, 3 \ldots\}$, denoted by $\mathbb{N}$
- The set of positive integers $\{1, 2, 3, \ldots\}$, denoted by $\mathbb{Z}^+$
- The set of prime numbers $\{2, 3, 5, 7, 11, 13, \ldots\}$, denoted by $\mathbb{P}$

"Elementary number theory" means the part of number theory that does not require heavy background in pure mathematics. But elementary does not mean easy!! There are many extremely hard problems in elementary number theory, for example the following:

**Problem 1.** Find all solutions to the following equation:

$$a^{(b^2)} = b^a$$

where $a$ and $b$ are positive integers.

This problem can be solved using only some calculus and really basic properties of the integers (such as the Fundamental Theorem of Arithmetic, see below), but it is still a very difficult problem!
In this part of the course, we will prove most of the theorems we state, with the aim of making you familiar with rigorous mathematical proofs. Number theory is a good area for starting to learn about proofs, since most proofs are short and not to hard to understand. However, we will not prove every theorem, because of our limited time, and because I don't want to torment you with proofs that don't give any particular insights. You are expected to:

- Understand and remember the statement of every theorem
- Be able to use the theorems for computations in concrete examples, such as the exercises of section 2.2 and 2.3 below
- For the final exam, be able to prove the theorems that are proved in these printed lecture notes (however, if you only aim for a passing grade, it should not be necessary to know the proofs)

## 2.2 Division, factorization and prime numbers

**Definition 6.** Let $a$ and $b$ be integers. If there exists an integer $m$ such that $b = ma$, then we say that $a$ *divides* $b$, or that $a$ is a *divisor* of $b$, or that $b$ is a *multiple* of $a$, or that $b$ is *divisible* by $a$. We write this as $a|b$.

For example, 5 divides 15, and 6 divides 12. In other words, 15 is a multiple of 5 and 12 is a multiple of 6.

**Example 1.** List all the positive divisors of 6. Answer: 1, 2, 3, 6.

**Example 2.** List all the positive divisors of 11. Answer: 1, 11.

**Example 3.** List all the positive divisors of 32. Answer: 1, 2, 4, 8, 16, 32.

### 2.2.1 Prime numbers

**Definition 7.** Let $a > 1$ be an integer. We say that $a$ is a *prime number* if has exactly two positive divisors, namely 1 and $a$. We say that $a$ is *composite* if it is not prime.

The number 1 is neither prime nor composite.
There is a simple method for listing the prime numbers up to any given size. This method is called Eratosthenes sieve. It goes as follows:

1. Write down the numbers 2, 3, 4, ... as far as you like.
2. Draw a circle around the number 2, and cross out all larger multiples of 2, that is 4, 6, 8, ...
3. Take the smallest untouched number in the list. Draw a circle around it, and cross out all larger multiples of it.
4. Repeat step 3 until you come to the end of the list.
5. Now all the prime numbers have a circle, and the composite numbers are crossed.

If you try this, you will see that the first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$$

### 2.2.2 Quotient and remainder

Now let's discuss the concepts of quotient and remainder. You have probably seen this a very long time ago, in primary school. For example, when we divide 17 by 5, the quotient is 3 and the remainder is 2.

**Definition 8.** Let $a, b$ be positive integers. In the division $\frac{a}{b}$, the *quotient* is the largest number $q$ such that $a \geq bq$. We denote it by $q$ or $q(a, b)$. The *remainder* is the number $(a - bq)$, denoted by $r$ or $r(a, b)$.

**Example 4.** In the division $\frac{10}{3}$, the quotient is 3, and the remainder is 1. Hence $q(10,3) = 3$ and $r(10,3) = 1$.

**Example 5.** In the division $\frac{24}{6}$, the quotient is 4, and the remainder is 0. Hence $q(24,6) = 4$ and $r(24,6) = 0$.

**Example 6.** In the division $\frac{19}{5}$, the quotient is 3, and the remainder is 4.

**Example 7.** In the division $\frac{1983}{179}$, the quotient is 11, and the remainder is 14.

### 2.2.3 GCD and LCM

**Definition 9.** When $a$ and $b$ are integers, not both zero, we write $GCD(a,b)$ for the greatest common divisor of $a$ and $b$, that is the largest positive integer that divides both $a$ and $b$. In the case where $a$ and $b$ are both zero, we define $GCD(a,b)$ to be 0.

**Example 8.** $GCD(15,12) = 3$. $GCD(24,42) = 6$. $GCD(19,28) = 1$.

**Example 9.** $GCD(-12,-8) = 4$. $GCD(0,35) = 35$. $GCD(-11,0) = 11$.

**Definition 10.** If $GCD(a,b) = 1$, we say that $a$ and $b$ are *coprime*.

**Definition 11.** When $a$ and $b$ are nonzero integers, we write $LCM(a,b)$ for the least common positive multiple of $a$ and $b$, that is the smallest positive number that has both $a$ and $b$ as divisors. If $a$ or $b$ (or both) equal zero, we define $LCM(a,b)$ to be zero.

**Example 10.** $LCM(6,7) = 42$. $LCM(8,-12) = 24$. $LCM(0,27) = 0$.

The best way of finding the $GCD$ of two numbers is to use Euclid's algorithm.

**Algorithm 1** (Euclid's algorithm)**.** Suppose that $a$ and $b$ are positive integers, and that we want to find $GCD(a,b)$. The idea of Euclid's algorithm is to produce a decreasing sequence of positive integers, such that the last nonzero number in the sequence is equal to $GCD(a,b)$. We start with $a$ and $b$, and then we compute remainders.

1. Let $m_1$ be the largest of $a$ and $b$
2. Let $m_2$ be the smaller of $a$ and $b$
3. Let $m_3 = r(a,b)$.
4. Continue like this, putting $m_{k+1} = r(m_{k-1}, m_k)$.
5. The last nonzero number in the sequence is $GCD(a,b)$.

Let's do one example:

**Example 11.** Let's compute $GCD(1806, 3174)$. We get the following sequence:

$$\begin{aligned} m_1 &= 3174 \\ m_2 &= 1806 \\ m_3 &= r(3174, 1806) = 1368 \\ m_4 &= r(1806, 1368) = 438 \\ m_5 &= r(1368, 438) = 54 \\ m_6 &= r(438, 54) = 6 \\ m_7 &= r(54, 6) = 0 \end{aligned}$$

so we get $GCD(1806, 3174) = 6$.

The following formula is useful when computing the $LCM$ of two integers. Since we have a method for finding $GCD$, we can use it to find $LCM$.

**Theorem 2.** For any positive integers $a$ and $b$, we have

$$GCD(a, b) \cdot LCM(a, b) = a \cdot b$$

*Proof.* This follows immediately from the alternative way of thinking about $GCD$ and $LCM$, discussed after the Fundamental Theorem of Arithmetic below. □

**Example 12.** We want to compute $LCM(1254, 779)$. Using Euclid's algorithm, we find that $GCD(1254, 779) = 19$. From the above theorem, we can compute

$$LCM(1254, 779) = \frac{1254 \cdot 779}{19} = 51414$$

### 2.2.4 Factorization

Now we'll talk about factorization of integers. You have probably seen before that every composite number can be factored into prime numbers. Some examples:

**Example 13.** $39 = 3 \cdot 13$

**Example 14.** $70 = 2 \cdot 5 \cdot 7$

**Example 15.** $686 = 2 \cdot 7 \cdot 7 \cdot 7$ (we usually write this as $2 \cdot 7^3$)

**Example 16.** $3762 = 2 \cdot 3^2 \cdot 11 \cdot 19$

There is only one way to factor an integer (up to the order of the factors). This is one of the most important statements of Elementary number theory:

**Theorem 3** (Fundamental Theorem of Arithmetic)**.** Every positive integer $n > 1$ can be written in a unique way as a product

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1 < p_2 < \ldots < p_k$ are primes and $e_i$ is a positive integer for every $i$.

*Proof.* The proof uses a method called *induction*. We will introduce this method later, and perhaps also give the proof of this theorem, if we have time. □

More examples:

**Example 17.** The prime factorization of 24 is $2^3 \cdot 3$.

**Example 18.** The prime factorization of 744 is $2^3 \cdot 3 \cdot 31$.

**Example 19.** The prime factorization of 18095 is $5 \cdot 7 \cdot 11 \cdot 47$.

**Example 20.** The prime factorization of 1862 is $2 \cdot 7^2 \cdot 19$.

Of, course, to find the factorization of large numbers it is most convenient to use a computer. If you feel that factoring integers is boring or meaningless, you may be interested in the following: If you can find the prime factorization of the following integer:

74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359

then you will be awarded a sum of US$ 30,000 from a research institute in the USA. Later in the course we will explain why someone would pay so much just for a factorization of a large number.
A natural question is the following: How do we determine whether a given number, for example 109, is prime or not? For large numbers, this is a difficult question, but for small numbers, we can use one of two simple methods. We can use either the Eratosthenes sieve (see above) or we can use the following fact:

**Theorem 4.** If a positive integer $n$ is composite, then it has a prime factor $p$ such that $p \leq \sqrt{n}$.

*Proof.* Let $p$ be the smallest prime factor of $n$. Then we have $n = p \cdot m$ for some positive integer $m$. The number $m$ can not be equal to 1, because that would imply $n = p$, which contradicts the hypothesis that $n$ is composite. Any prime factor of $m$ is at least as large as $p$, so we must have $p \leq m$. Hence $p^2 \leq p \cdot m$, that is $p^2 \leq n$, which implies $p \leq \sqrt{n}$. We have proved that the smallest prime factor of $n$ is smaller than or equal to $\sqrt{n}$. □

To check whether a given integer $n$ is prime or not, we could check, for each prime number smaller than $n$, whether $p$ divides $n$ or not. If no such prime divides $p$, we could conclude that $n$ is itself prime. Because of the above theorem, it is actually sufficient to only try all prime numbers up to $\sqrt{n}$.

**Example 21.** Is 109 a prime number or not? To find the answer, we must check if 109 is divisible by some prime number smaller than $\sqrt{109} = 10.44\ldots$. These primes are 2, 3, 5, and 7. Checking shows that none of them divides 109, so the number 109 is a prime number.

**Example 22.** Is 437 a prime number or not? To find the answer, we must check all primes up to $\sqrt{437} = 20.9\ldots$. None of 2, 3, 5, 7, 11, 13, 17 divides 437, but we find that 19 divides 437, so it is not a prime.

### 2.2.5 Some basic but useful facts

Let $n$ be a positive integer

- $2|n$ if and only if 2 divides the last digit of $n$
- $5|n$ if and only if 5 divides the last digit of $n$
- $3|n$ if and only if 3 divides the sum of the digits of $n$
- $11|n$ if and only if 11 divides the alternating sum of the digits of $n$

There are also similar rules for 7 and 13, but they are slightly more complicated, and we will not need them.

**Example 23.** The number 32109 is not divisible by 2 or 5, since the last digit is 9. It is divisible by 3, because the sum of the digits is 15. It is also divisible by 11, because the alternating sum of the digits is

$$3 - 2 + 1 - 0 + 9 = 11$$

which is of course divisible by 11.

### 2.2.6 Another way of thinking about GCD and LCM

Let $a$ and $b$ be two positive integers. Consider the set of all primes occurring in the prime factorizations of these two integers. Call these primes $q_1, q_2, \ldots q_n$. Then we have

$$a = q_1^{e_1} \cdots q_n^{e_n}$$

and also

$$b = q_1^{f_1} \cdots q_n^{f_n}$$

for some natural numbers $e_i$ and $f_i$. Some of these $e_i$ and $f_i$ might be zero, for example $e_1$ will be zero if $q_1$ does not occur in the factorization of $a$.
When will it be the case that $a$ divides $b$? Using the above notation, it will be the case exactly if $e_i \leq f_i$ for each $i$. For example, the number $18 = 2 \cdot 3^2$ divides the number $252 = 2^2 \cdot 3^2 \cdot 7$, because each exponent in the factorization of 18 is smaller than or equal to the corresponding exponent in the factorization of 252.
We continue to use the notation introduced above, and we want to find the $GCD$ and $LCM$ of $a$ and $b$. We define new numbers as follows:

$$\begin{aligned} g_i &= \min(e_i, f_i) \\ m_i &= \max(e_i, f_i) \end{aligned}$$

(this means that $m_i$ is the largest of $e_i$ and $f_i$, and $g_i$ is the smallest.)
With this notation, we have

$$GCD(a, b) = q_1^{g_1} \cdots q_n^{g_n}$$

and

$$LCM(a, b) = q_1^{m_1} \cdots q_n^{m_n}$$

Some examples will make this clearer.

**Example 24.** Take $a = 1176 = 2^3 \cdot 3 \cdot 7^2$ and $b = 3276 = 2^2 \cdot 3^2 \cdot 7 \cdot 13$. Then, with the above notation, we have

$$q_1 = 2, \quad q_2 = 3, \quad q_3 = 7, \quad q_4 = 13$$

$$e_1 = 3, \quad e_2 = 1, \quad e_3 = 2, \quad e_4 = 0$$

$$f_1 = 2, \quad f_2 = 2, \quad f_3 = 1, \quad f_4 = 1$$

$$g_1 = 2, \quad g_2 = 1, \quad g_3 = 1, \quad g_4 = 0$$

$$m_1 = 3, \quad m_2 = 2, \quad m_3 = 2, \quad m_4 = 1$$

and we can conclude that

$$GCD(a, b) = 2^2 \cdot 3 \cdot 7 = 84, \qquad LCM(a, b) = 2^3 \cdot 3^2 \cdot 7^2 \cdot 13 = 45864$$

**Example 25.** Take $a = 875 = 5^3 \cdot 7$ and $b = 6885 = 3^4 \cdot 5 \cdot 17$. Then, with the above notation, we have

$$q_1 = 3, \quad q_2 = 5, \quad q_3 = 7, \quad q_4 = 17$$

$$e_1 = 0, \quad e_2 = 3, \quad e_3 = 1, \quad e_4 = 0$$

$$f_1 = 4, \quad f_2 = 1, \quad f_3 = 0, \quad f_4 = 1$$

$$g_1 = 0, \quad g_2 = 1, \quad g_3 = 0, \quad g_4 = 0$$

$$m_1 = 4, \quad m_2 = 3, \quad m_3 = 1, \quad m_4 = 1$$

and we can conclude that

$$GCD(a, b) = 5, \qquad LCM(a, b) = 3^4 \cdot 5^3 \cdot 7 \cdot 17 = 1204875$$

### 2.2.7 Exercises

**E71** Find the quotient and the remainder in the division $\frac{31}{6}$.
**E72** Find the quotient and the remainder in the division $\frac{399}{12}$.
**E73** Find the quotient and the remainder in the division $\frac{504}{84}$.
**E74** Find the prime factorization of the following integers: 9, 21, 39, 51, 53, 72, 88, 91.
**E75** Find the prime factorization of the following integers: 18513, 9288, 103350.
For each of the statements E76 to E95, determine whether it is true or false:
**E76** $10|24$
**E77** $24|10$
**E78** $7|49$
**E79** 8 is a multiple of 4
**E80** 11 is a multiple of 33
**E81** 37 is a multiple of 37
**E82** 18 divides 6
**E83** 5 is a divisor of 25
**E84** 6 is a divisor of 9
**E85** $49|7$
**E86** 106 divides 0
**E87** 0 divides 106
**E88** 0 divides 0
**E89** 1 is a divisor of 12
**E90** 1 is a multiple of 0
**E91** 8 is a multiple of 1
**E92** 0 is a multiple of 1
**E93** 0 is a multiple of 129
**E94** 0 is a multiple of 1000
**E95** 27 is divisible by 9

**E96** List the positive divisors of 25.
**E97** List the positive divisors of 18.
**E98** List the first few positive multiples of 7.
**E99** List the first few positive multiples of 23.
**E100** List the multiples of 0.
**E101** Use Eratosthenes sieve to list all primes smaller than 100. How many are they?
**E102** Which of the following numbers are prime: 10, 37, 51, 72, 101, 173, 309, 1002, 10235, 13273.
Compute the following quotients and remainders:
**E103** $q(180, 18)$.
**E104** $r(180, 18)$.
**E105** $q(99, 7)$.
**E106** $r(99, 7)$.
**E107** $q(846, 19)$.
**E108** $r(846, 19)$.
**E109** $q(3477, 2190)$.
**E110** $r(3477, 2190)$.
**E111** $q(6991, 1885)$.
**E112** $r(6991, 1885)$.
Compute the following:
**E113** $GCD(60, 90)$.
**E114** $LCM(60, 90)$.
**E115** $GCD(192, 318)$.
**E116** $LCM(192, 318)$.
**E117** $GCD(1992, 432)$.
**E118** $GCD(5005, 11011)$.
**E119** $GCD(0, 58)$.
**E120** $LCM(99, 0)$.
**E121** $GCD(0, 0)$.
**E122** $GCD(192, 318)$.
**E123** $GCD(2118, 713)$.
**E124** Are 218 and 5444 coprime?
**E125** Are 4730 and 13671 coprime?.
**E126** Find $GCD(79507, 5547)$ without using Euclid's algorithm. You may use the fact that $79507 = 43^3$ and $5547 = 3 \cdot 43^2$.
Find the prime factorization of the following six integers:
**E127** 343
**E128** 3280
**E129** 4114
**E130** 10989
**E131** 2592
**E132** 17303
**E133** Compute $GCD(10989, 17303)$.

### 2.2.8 Problems

**P7** Prove that "$a$ divides $b$" is a reflexive and transitive relation on $\mathbb{Z}$.

Try to determine whether the following two statements are true or false. You may begin by checking whether the statement holds or not for some small values of $n$.

**P8** For all $n \in \mathbb{Z}^+$, the following formula holds:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

**P9** Let $n$ be an integer. Then $n^2 + n + 17$ is always a prime number.

## 2.3 Ideals

We shall now discuss certain subsets of $\mathbb{Z}$ which are very important.

**Definition 12.** An *ideal* is a subset of $\mathbb{Z}$ of the following form:

$$\{x \in \mathbb{Z} \mid x \text{ is a multiple of } m\}$$

for some integer $m$. We write $\langle m \rangle$ for this ideal.

**Example 26.** The ideal $\langle 5 \rangle$ is the set

$$\{\ldots, -10, -5, 0, 5, 10, 15, 20, \ldots\}$$

**Example 27.** The ideal $\langle 12 \rangle$ is the set

$$\{\ldots, -24, -12, 0, 12, 24, 36, 48, \ldots\}$$

**Example 28.** The ideal $\langle 0 \rangle$ is the set $\{0\}$. This ideal is called the *zero ideal*.

Note that every ideal except the zero ideal is an infinite set, containing both negative and positive numbers, and also the number zero.

**Definition 13.** For a nonzero ideal, we define the *generator* of the ideal to be the smallest positive element of the ideal. The generator of the zero ideal is defined to be the number 0.

**Example 29.** The generator of the ideal

$$\{\ldots, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$$

is the number 3.

Note that the generator is defined so that any ideal is the set of all multiples of its generator.

**Theorem 5.** A nonempty subset $M$ of $\mathbb{Z}$ is an ideal if and only if it is closed under subtraction. (This last condition means that whenever $n$ and $k$ are in $M$, then $(n-k)$ is also in $M$.)

*Proof.* Omitted. □

**Definition 14.** Let $a, b \in \mathbb{Z}$. A *linear combination* of $a$ and $b$ is an integer of the form $xa + yb$ for some $x, y \in \mathbb{Z}$. The set of all linear combinations of $a$ and $b$ is denoted by $\langle a, b \rangle$.

**Example 30.** Some examples of linear combinations of $a$ and $b$:

$$2a + 3b\ , \quad 10a - b\ , \quad b\ , \quad -a - 100b$$

**Example 31.** 8 is a linear combination of 12 and 26, because we have $8 = 5 \cdot 12 - 2 \cdot 26$. Another example: 1 is a linear combination of 10 and 7, because we have $1 = 5 \cdot 10 - 7 \cdot 7$.

The set $\langle a, b \rangle$ is the set of all integers that can be reached from 0, using only jumps of length $a$ and $b$. For example, the last example shows that making five jumps of length 12 in the positive direction and then two jumps of length 26 in the negative direction takes us to the number 8. Similarly, we can reach 1 by jumping five jumps of length 10 in the positive direction, and then seven jumps of length 7 in the negative direction.

**Theorem 6.** Let $a$ and $b$ be two integers. Then the set $\langle a, b \rangle$ is an ideal.

*Proof.* It is enough to show that the set is closed under subtraction. So let $n$ and $k$ be two elements of $\langle a, b \rangle$. Then we have

$$n = x_1 a + y_1 b$$
$$k = x_2 a + y_2 b$$

for some integers $x_1, x_2, y_1, y_2$. But we see that

$$n - k = (x_1 - x_2) \cdot a + (y_1 - y_2) \cdot b$$

which shows that $(n-k)$ is also a linear combination of $a$ and $b$. Hence we can conclude that $\langle a, b \rangle$ is closed under subtraction. □

**Theorem 7.** The generator of $\langle a, b \rangle$ is equal to $GCD(a, b)$.

*Proof.* We consider two different cases, and use a separate argument for each case. In the proof of Case 2, we use the following three facts:

- If $d|a$ and $d|b$, then $d$ divides every linear combination of $a$ and $b$.
- If $d|a$ and $d|b$, then $d$ also divides $GCD(a, b)$.

- If two positive integers divide each other, then they must be equal.

**Case 1: $\langle a, b\rangle$ is the zero ideal.** This means that every linear combination of $a$ and $b$ is equal to 0. Since $a$ is a linear combination of $a$ and $b$, we see that $a = 0$. For the same reason, $b = 0$. So from the definition of $GCD$, we see that $GCD(a, b) = 0$. Clearly this is equal to the generator of $\langle a, b\rangle$.
**Case 2: $\langle a, b\rangle$ is not the zero ideal.** Let $d$ be the generator of $\langle a, b\rangle$. It is a positive number. Since it is a linear combination of $a$ and $b$, there are integers $x, y$ such that $d = xa + by$. By definition of $GCD$, the number $GCD(a, b)$ divides $a$, and it also divides $b$. Hence it must divide $d$ (by the first fact above).
The set $\langle a, b\rangle$ is the set of all multiples of the generator $d$. Since $a$ and $b$ are elements of $\langle a, b\rangle$, both $a$ and $b$ are multiples of $d$. Therefore, (by the second fact above), $d$ must divide $GCD(a, b)$. Now $d$ and $GCD(a, b)$ are positive integers dividing each other, so they must be equal (third fact above). □

**Theorem 8** (Bezout's theorem)**.** Let $a, b \in \mathbb{Z}$. Then $GCD(a, b)$ can be written as a linear combination of $a$ and $b$.

*Proof.* The previous theorem shows that $GCD(a, b)$ is an element of $\langle a, b\rangle$. □

**Theorem 9.** The intersection of two ideals is an ideal.

(I forgot to prove this in class, but include it here for completeness.)

*Proof.* Let $I$ and $J$ be two ideals. Then they are both closed under subtraction, and they both contain the number 0. Let $n$ and $k$ are any elements of the intersection $I \cap J$. Then because $n$ and $k$ are in $I$, the difference $(n - k)$ is also an element of $I$. For the same reason we see that $(n - k)$ is in $J$. But this implies that $(n - k)$ is an element of $I \cap J$. Hence $I \cap J$ is closed under subtraction , so it is an ideal. (It is nonempty because it contains the number 0.) □

**Theorem 10.** The generator of $\langle a\rangle \cap \langle b\rangle$ is equal to $LCM(a, b)$.

*Proof.* Again we consider two different cases.
**Case 1: At least one of $a$ and $b$ equals zero.**
In this case one of the sets $\langle a\rangle$ and $\langle b\rangle$ (or both) is the zero ideal. Hence the intersection $\langle a\rangle \cap \langle b\rangle$ is the zero ideal, and its generator is 0. We also have $LCM(a, b) = 0$, by definition of $LCM$.
**Case 2: $a$ and $b$ are both nonzero.**
We know that

- $\langle a\rangle$ is the set of all multiples of $a$
- $\langle b\rangle$ is the set of all multiples of $b$

Hence the intersection of the two ideals is the set of integers that are a multiple of $a$ *and* a multiple of $b$. Since $LCM(a,b)$ has this property, it is an element of $\langle a\rangle \cap \langle b\rangle$. We must show that $LCM(a,b)$ is actually the *smallest* positive element of $\langle a\rangle \cap \langle b\rangle$. But this follows immediately from the definition of $LCM$. □

**Theorem 11** ("To divide is to contain")**.** Let $a$ and $b$ be integers. Then $a|b$ if and only if $\langle a\rangle \supseteq \langle b\rangle$.

*Proof.* There are two things to prove.
**Part 1:** $a|b \implies \langle a\rangle \supseteq \langle b\rangle$.
Suppose that $a$ divides $b$. Then $b = ac$ for some $c$. Hence every multiple of $b$ is also a multiple of $a$. Hence the set of all multiples of $b$ is a subset of the set of all multiples of $a$, so $\langle a\rangle \supseteq \langle b\rangle$.
**Part 2:** $\langle a\rangle \supseteq \langle b\rangle \implies a|b$.
Suppose that $\langle a\rangle \supseteq \langle b\rangle$. Since $b$ is an element of $\langle b\rangle$, it must then also be an element of $\langle a\rangle$. This means that $b$ is a multiple of $a$, that is $a|b$. □

### 2.3.1 Exercises

Are the following three sets examples of ideals?
**E134** The set of positive integers.
**E135** The set of even integers.
**E136** The set of prime numbers.
**E137** Write down some elements of $\langle 9\rangle$.
**E138** Write down some elements of $\langle 7\rangle \cap \langle 3\rangle$.
**E139** What is the generator of $\langle 191\rangle$?
**E140** What is the generator of $\langle 6\rangle \cap \langle 9\rangle$?
**E141** How many elements of the ideal $\langle 7\rangle$ are positive and smaller than 55?
**E142** Is 14 a linear combination of 2 and 6 ?
**E143** Is 9 a linear combination of 2 and 6 ?
Compute the generators of the following ideals:
**E144** $\langle 4, 9\rangle$
**E145** $\langle 114, 216\rangle$
**E146** $\langle 50700, 8424\rangle$
**E147** $\langle 4\rangle \cap \langle 3\rangle$
**E148** $\langle 16\rangle \cap \langle 18\rangle$
Use the previous exercises to answer the following questions:
**E149** Is 17 a linear combination of 4 and 9?
**E150** Is 18911 a linear combination of 4 and 9?
**E151** Is 18 a linear combination of 114 and 216?
**E152** Is 2 a linear combination of 114 and 216?
**E153** Is 258 a linear combination of 114 and 216?
**E154** Is 1092 a linear combination of 8424 and 50700?

## 2.4 Answers and solutions

### 2.4.1 Exercises

**E71** $q = 5, \quad r = 1$
**E72** $q = 33, \quad r = 3$
**E73** $q = 6, \quad r = 0$
**E74** $9 = 3 \cdot 3$. $21 = 3 \cdot 7$. $39 = 3 \cdot 13$. $51 = 3 \cdot 17$. $53 = 53$ (a prime number). $72 = 2^3 \cdot 3^2$. $88 = 2^3 \cdot 11$. $91 = 7 \cdot 13$.
**E75** $18513 = 3^2 \cdot 11^2 \cdot 17$. $9288 = 2^3 \cdot 3^3 \cdot 43$. $103350 = 2 \cdot 3 \cdot 5^2 \cdot 13 \cdot 53$.
**E76** False. **E77** False. **E78** True. **E79** True. **E80** False. **E81** True. **E82** False. **E83** True. **E84** False. **E85** False. **E86** True. **E87** False. **E88** True. **E89** True. **E90** False. **E91** True. **E92** True. **E93** True. **E94** True. **E95** True.
**E96** 1, 5, 25
**E97** 1, 2, 3, 6, 9, 18
**E98** 7, 14, 21, 28, ...
**E99** 23, 46, 69, 92, ...
**E100** 0 is the only multiple of 0.
**E101** There are 25 such primes, namely 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.
**E102** Only 37, 101 and 173 are prime.
**E103** 10. **E104** 0. **E105** 14. **E106** 1. **E107** 44. **E108** 10. **E109** 1. **E110** 1287. **E111** 3. **E112** 1336. **E113** 30. **E114** 180. **E115** 6. **E116** 10176. **E117** 24. **E118** 35856. **E119** 58. **E120** 0. **E121** 0. **E122** 6. **E123** 1.
**E124** No
**E125** Yes
**E126** The answer is $43^2 = 1849$
**E127** $7^3$
**E128** $2^4 \cdot 5 \cdot 41$
**E129** $2 \cdot 11^2 \cdot 17$
**E130** $3^3 \cdot 11 \cdot 37$
**E131** $2^5 \cdot 3^4$
**E132** $11^3 \cdot 13$
**E133** 11
**E134** No
**E135** Yes
**E136** No
**E137** $0, 9, 18, 27, \ -9, \ -18$
**E138** $-21, 0, 21, 42, 63, 84$
**E139** 191
**E140** 18
**E141** 7 elements
**E142** Yes

**E143** No
**E144** 1
**E145** 6
**E146** 156
**E147** 12
**E148** 144
**E149** Yes. **E150** Yes. **E151** Yes. **E152** No. **E153** Yes. **E154** Yes.

### 2.4.2 Problems

**P7** To prove that this relation is reflexive, we must prove that $a$ divides $a$ for every $a$. That is, we must prove that for every $a$, there is an integer $m$ such that $a = ma$. Obviously, the integer 1 has this property, for every $a$.
To prove that the relation is transitive, suppose that $a|b$ and $b|c$. Then, from the definition, there exist integers $m_1$ and $m_2$ such that $b = m_1 a$ and $c = m_2 b$. But this implies that

$$c = m_2 b = m_2 m_1 a$$

which shows that $a$ divides $c$.
**P8** Make a table, as we did before in class, with one column for the sum of the first $n$ integers, and another column for the number $\frac{n(n+1)}{2}$. You will see that the two columns agree for $n = 1$, $n = 2$, $n = 3$, $n = 4$ and so on. In fact this formula is true for all $n$. The proof uses a method called induction, and we will prove the formula later.
**P9** Again, you can compute the value of $n^2 + n + 17$ for small values of $n$. You will see that you get a prime number for $n = 0$, $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$, $n = 6$, and also for small negative values of $n$. This might lead us to believe that we always get a prime number. However, try the number $n = 17$. Do we get a prime number in this case?

## SMA205, HOME ASSIGNMENT 1

Deadline for hand-in: Monday, Dec 4.

Please write your full name here:

---

and your registration number here: __ __ __ $\underbrace{\_\_\ \_\_\ \_\_\ \_\_}_{x}$ __ __

Let $x$ be the four-digit number indicated. For example, if your registration number is I20 2477 04, then $x = 2477$.

1. Is the following formula correct or not, for all positive integers $n$?

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

   Prove your answer! (5 marks)

2. Let $a, b, \in \mathbb{Z}$. Prove the following statement:

   If $a^2 + b^2 \equiv 0 \pmod 3$, then $ab \equiv 0 \pmod 3$.

   (3 marks)

3. Find the prime factorization of the number $x$.

   Answer: _____
   (2 marks)

## 2.5 Congruences

For this section, we think of $m$ as a fixed positive integer.

**Definition 15.** We say that $a$ is *congruent* to $b$ modulo $m$, and we write

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

if $m$ divides $(a - b)$.

IMPORTANT NOTE: All the following statements are equivalent:

- $a \equiv b \pmod{m}$
- $a$ and $b$ give the same remainder when divided by $m$
- $a$ can be written as $b + km$ for some integer $k$
- $a$ can be reached from $b$ (and vice versa) by jumping only jumps of length $m$
- $(a - b)$ is an element of the ideal $\langle m \rangle$

Switching between these different formulations will help you solve most problems concerning congruence questions.

**Theorem 12.** The relation $a \equiv b \pmod{m}$ is an equivalence relation on $\mathbb{Z}$.

*Proof.* This should be obvious from the 2nd point above. □

Congruence behave in many ways just like equality. This is very useful in arguments with congruences. To be precise, the following rules hold. (The proofs of these rules is not the important thing, the important thing is that you can use the rules in calculations and arguments.)

**Theorem 13** (Rules for congruences)**.** If we have two congruences mod $m$, we may add them, multiply them, and subtract them. In other words, suppose that

$$a \equiv b \pmod{m} \qquad \text{and} \qquad c \equiv d \pmod{m}$$

Then the following holds:

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ ac &\equiv bd \pmod{m} \\ a - c &\equiv b - d \pmod{m} \end{aligned}$$

*Proof.* Our hypothesis is that $m$ divides $(a - b)$ and $m$ also divides $(c - d)$. Then $m$ must divide $(a - b) + (c - d) = (a + c) - (b + d)$, which gives the first congruence. Similar easy arguments prove the second and third congruence. □

**Theorem 14** (More rules for congruences)**.** We may multiply both sides of a congruence by an integer, and we may raise both sides of a congruence to a power. More precisely, suppose that $a \equiv b \pmod{m}$. Then the following holds:

$$na \equiv nb \pmod{m}$$

for every integer $n$, and

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

for every positive integer $n$.

*Proof.* This follows from the previous theorem. Add the congruence $a \equiv b \pmod{m}$ to itself $n$ times to get the $na \equiv nb \pmod{m}$, and multiply it $n$ times to get $a^n \equiv b^n \pmod{m}$. □

**Theorem 15** (Cancellation law)**.** If $ac \equiv bc \pmod{m}$ and $GCD(m, c) = 1$, then $a \equiv b \pmod{m}$.

*Proof.* The first part of the hypothesis says that $m|(ac - bc)$, that is, $m$ divides $c(a - b)$. Since the second part of the hypothesis says that $m$ has no prime factor in common with $c$, we can conclude that $m$ must divide $(a - b)$. □

Let us now prove a few simple theorems, to show how congruences can be used. The important thing in these examples is not the statement of the theorem, but the method of proof, using congruences.

**Theorem 16.** Every odd square gives the remainder 1 when divided by 4.

*Proof.* (Recall that a square is an integer of the form $n^2$ for some $n$. Hence the odd squares are 1, 9, 25, 49 and so on.) If a square $n^2$ is odd, then clearly the number $n$ must also be odd. This implies that $n$ gives remainder 1 or 3 when divided by 4. We consider each of these cases.

**Case of remainder 1**

In this case, we have

$$n \equiv 1 \pmod{4}$$

Squaring both sides gives

$$n^2 \equiv 1 \pmod{4}$$

which means that $n^2$ gives remainder 1 when divided by 4.

**Case of remainder 3**

In this case, we have

$$n \equiv 3 \pmod{4}$$

Squaring both sides gives

$$n^2 \equiv 9 \pmod{4}$$

and since $9 \equiv 1 \pmod{4}$ we have $n^2 \equiv 1 \pmod{4}$. □

As another illustration of the use of congruences, we prove the following fact:

**Theorem 17.** Let $n$ be a positive integer. Then 3 divides the sum of the digits of $n$ if and only if 3 divides $n$.

*Proof.* Suppose that the digits of $n$ are $a_k a_{k-1} \dots a_1 a_0$, where $0 \leq a_j \leq 9$ for each $j$. (For example, if $n = 924$, then $a_2 = 9$, $a_1 = 2$ and $a_0 = 4$.) Since $n$ is written in base 10, this means that

$$n = \sum_{j=0}^{k} a_j \cdot 10^j = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$$

Of course, the digit sum of $n$ is the number

$$\sum_{j=0}^{k} a_j$$

The crucial step of the proof is to observe the following:

$$a_j \cdot 10^j \equiv a_j \pmod 3 \tag{1}$$

To prove the congruence (1), we can take the congruence

$$10 \equiv 1 \pmod 3$$

and raise each side to the power $j$, and then multiply both sides by $a_j$. Now we take the congruence (1) and sum it over all $j$. This gives us

$$\sum_{j=0}^{k} a_j \cdot 10^j \equiv \sum_{j=0}^{k} a_j \pmod 3$$

This is the same as

$$n \equiv \sum_{j=0}^{k} a_j \pmod 3$$

which means that $n$ is congruent to the digit sum of $n$, mod 3. This implies that $n$ is divisible by 3 if and only if its digit sum is divisible by 3. □

Now let us prove two important theorems about existence of solutions to certain congruences.

**Theorem 18.** Let $a, b$ be two integers. Consider the congruence

$$ax \equiv b \pmod m$$

This congruence is solvable (i.e. their exists an integer $x$ satisfying the congruence) if and only if $b$ is a multiple of $GCD(a, m)$.

*Proof.* First we assume that their exists an $x$ satisfying the congruence. Then $(b - ax)$ is a multiple of $m$. This implies

$$b - ax = km$$

for some integer $k$. This implies $b = ax + km$, so $b$ is a linear combination of $m$ and $a$. Hence $b \in \langle a, m \rangle$, which implies that $b$ is a multiple of $GCD(a, m)$. Now we have to prove the converse. Assume that $b$ is a multiple of $GCD(a, m)$. Then $b \in \langle a, m \rangle$, so

$$b = ax + my$$

for some integers $x$ and $y$. For this particular $x$, we see that $b - ax$ is a multiple of $m$, so $x$ satisfies the congruence of the theorem. □

**Theorem 19** (Chinese remainder theorem)**.** Let $a, b \in \mathbb{Z}$, and let $m$ and $n$ be positive coprime integers. Then there exists $z \in \mathbb{Z}$ such that

$$\begin{aligned} z &\equiv a \pmod{m} \\ z &\equiv b \pmod{n} \end{aligned}$$

*Proof.* Since $n$ and $m$ are coprime, we have $\langle m, n \rangle = \mathbb{Z}$. In other words, every integer is a linear combination of $m$ and $n$. Hence there are some integers $x$ and $y$ such that

$$a - b = xm + yn$$

Now let $z = a - xm$. This implies $z = b + yn$. Now it is obvious that $z$ satisfies the two congruences in the theorem. □

The last theorem of this section is a useful fact about primes.

**Theorem 20.** A prime $p > 3$ gives remainder 1 or 5 when divided by 6.

*Proof.* If we divide an integer by 6, the remainder is 0, 1, 2, 3, 4, or 5. Suppose $p$ is prime and greater than 3. Clearly $p$ cannot be even, so the remainder of $p$ when divided by 6 cannot be 0, 2, or 4. Also, the remainder cannot be 3, since this would imply that $p$ is divisible by 3, and hence not prime. Therefore the remainder must be 1 or 5. □

### 2.5.1 Exercises

For each of the statements E155 to E169, determine whether it is true or false:
**E155** $3 \equiv -3 \pmod{5}$
**E156** $12 \equiv 24 \pmod{24}$
**E157** $0 \equiv 0 \pmod{8}$
**E158** $9 \equiv 30 \pmod{7}$

**E159** $31 \equiv -26 \pmod 5$
**E160** $6 \equiv 132 \pmod{12}$
**E161** Every integer $n$ can be written either as $2k$ or as $2k+1$ for some integer $k$.
**E162** If $n \equiv 3 \pmod 5$, then $n^3 \equiv 4 \pmod 5$.
**E163** If $a \equiv b \pmod{16}$, then $a \equiv b \pmod 8$.
**E164** If $a \equiv b \pmod 5$, then $a \equiv b \pmod{10}$.
**E165** If $a \equiv b \pmod m$, then $-a \equiv -b \pmod m$.
**E166** If $x \equiv 3 \pmod m$, then $x + 4 \equiv 7 \pmod m$.
**E167** If $a \equiv b \pmod m$, then $a^2 \equiv b^3 \pmod m$.
**E168** If $2x \equiv 6 \pmod 4$, then $x \equiv 3 \pmod 4$.
**E169** If $3a \equiv 3b \pmod 7$, then $a \equiv b \pmod 7$.
**E170** What remainders can you get when dividing a square by 3?
**E171** What remainders can you get when dividing a square by 5?
**E172** Is the congruence $2x \equiv 7 \pmod 3$ solvable? If yes, can you find such an $x$?
**E173** Is the congruence $8x \equiv 6 \pmod{12}$ solvable? If yes, can you find such an $x$?
**E174** Is the congruence $9x \equiv 2 \pmod 6$ solvable? If yes, can you find such an $x$?
**E175** Is the congruence $3x \equiv 5 \pmod 8$ solvable? If yes, can you find such an $x$?
**E176** Is there an integer which gives the remainder 2 when divided by 5 and the remainder 3 when divided by 7? If yes, find such an integer.
**E177** Is there an integer which gives the remainder 1 when divided by 10 and the remainder 8 when divided by 9? If yes, find such an integer.
**E178** Is there an integer which gives the remainder 2 when divided by 6 and the remainder 3 when divided by 4? If yes, find such an integer.

### 2.5.2 Problems

**P10** Find all prime numbers such that $p^2 + 2$ is also a prime number.
**P11** Let $n$ be a positive integer. Prove that $n$ is congruent to the alternating digit sum of $n$, mod 11.
**P12** Prove that if $p > 3$ is a prime, then $24|(p^2 - 1)$.
**P13** Find an integer $x$ such that $38x \equiv 5 \pmod{17}$.
**P14** Is there a positive integer $n$ such that

$$n^2 \equiv n \pmod p$$

for every prime number $p$?

## 2.6 Induction proofs

An important method of proof, which is useful both in number theory and in many other parts of mathematics, is the method of *induction*. It can often be used to prove that a certain statement holds for all positive integers $n$. Let $S(n)$ denote a statement about the integer $n$. For example, $S(n)$ could be any of the following statements:

- $n$ is a prime number
- $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$
- $(5^{2n-1} + 1)$ is divisible by 6
- $(n^2 + n + 17)$ is a prime number
- A set with $n$ elements has $2^n$ subsets
- $n$ can be written as the sum of at most three prime numbers

Consider the first of these examples. In this case, $S(2)$ is a true statement, while $S(4)$ is a false statement. What do you think about the other statements? Are they true for all positive integers $n$, or only for some positive integers $n$, or perhaps false for all positive integers $n$?
If a statement is true for all positive integers $n$, one way of proving it might be by induction. The idea of an induction proof is the following: Let $S(n)$ be the statement to be proved for all positive integers $n$.

1. Prove that $S(1)$ is true (Base step)
2. Prove that $S(n)$ implies $S(n+1)$ (Induction step)

If we can prove both of these steps, we may conclude that $S(n)$ is true for all positive integers $n$ (this is called the Principle of Induction).
In most cases, the base step is the easy part and the induction step is the complicated part. However, you must never forget to do both steps, otherwise the proof is not valid! Let us now prove a few theorems to show how induction proofs work.

**Theorem 21.** For all positive integers $n$, the integer $(5^{2n-1} + 1)$ is divisible by 6.

*Proof.* We proceed by induction. The statement $S(n)$ is the statement of the theorem.
**Base step:** We compute, for $n = 1$:

$$5^{2n-1} + 1 = 6$$

The statement $S(1)$ therefore says that 6 is divisible by 6, which is of course true.
**Induction step:** Assume that $S(n)$ is true. The statement $S(n+1)$, that we must prove, says the following:

$5^{2(n+1)-1} + 1$ is divisible by 6.

Since $2(n+1) - 1$ is equal to $(2n+1)$, we must prove that

$5^{2n+1} + 1$ is divisible by 6.

How can be prove this? We must use the statement $S(n)$, which we assume to be true. Reformulating in terms of congruences, $S(n)$ says that

$$5^{2n-1} \equiv -1 \pmod 6$$

Multiplying both sides by 25, we get

$$5^{2n+1} \equiv -25 \pmod 6$$

and since $-25 \equiv -1 \pmod 6$, we can conclude that

$$5^{2n+1} \equiv -1 \pmod 6$$

which implies that $S(n+1)$ is true.
By the Principle of Induction we now know that $S(n)$ is true for all positive integers $n$. □

**Theorem 22.** Let $n$ be a positive integer. The sum of the first $n$ positive integers is equal to $\frac{n(n+1)}{2}$.

*Proof.* The statement $S(n)$ to be proved is the following statement:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

The statement $S(n+1)$ is the following:

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$$

Let's proceed by induction.
**Base step:** Consider the statement $S(n)$ for $n = 1$. In this case, we have

$$\sum_{k=1}^{n} k = 1$$

and

$$\frac{n(n+1)}{2} = 1$$

so the statement $S(1)$ is true.
**Induction step:** Assume that the statement $S(n)$ is true. We must use this to prove $S(n+1)$. The statement $S(n)$ says

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Now add $(n+1)$ to both sides of this equality. We get

$$\big(\sum_{k=1}^{n} k\big) + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

which is the same as

$$\sum_{k=1}^{n+1} k = \frac{n^2}{2} + \frac{n}{2} + n + 1$$

But the right hand side of this equality is equal to $\frac{(n+1)(n+2)}{2}$ (check this!) which means that we have proved the statement $S(n+1)$.
Now the Principle of Induction allows us to conclude that $S(n)$ is true for all $n$. □

**Theorem 23.** If $A$ is a set with $n$ elements, then $A$ has $2^n$ subsets.

*Proof.* Recall that we proved the following lemma in the lectures (we omit this proof here, as the important point is the induction proof):

**Lemma 1.** Let the finite set $A$ have one more element than the set $B$. Then $A$ has twice as many subsets as $B$.

Let us now the induction proof. The statement $S(n)$ is the statement of the theorem.
**Base step:** The statement $S(1)$ is true, because a set $A$ with one element has exactly two subsets: the empty set and the set $A$ itself.
**Induction step:** Assume that $S(n)$ is true. This means that a set with $n$ elements has $2^n$ subsets. By the lemma we can see that a set with $(n+1)$ elements has $2 \cdot 2^n$ subsets, that is $2^{n+1}$ subsets. Hence the statement $S(n+1)$ is also true.
Now the Principle of Induction allows us to conclude that $S(n)$ is true for all positive integers $n$. □

Let us again summarize the method of induction:

- In the base step, we prove that $S(1)$ is true
- In the induction step, we *assume* that $S(n)$ is true, and use this to prove that $S(n+1)$ is true

### 2.6.1 Exercises

**E179** Prove that $2^{3n} \equiv 1 \pmod 7$ for every positive integer $n$.
**E180** Prove that $3^n \equiv 3 \pmod 6$ for every positive integer $n$.

### 2.6.2 Problems

**P15** Try to find a formula for the sum of the first $n$ odd numbers.

For the last two problems, we define the *Fibonacci numbers* as follows:

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \qquad \text{for } n \geq 2 \end{aligned}$$

We can easily compute $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$ and so on.
**P16** Prove that $F_{3n}$ is even for every $n$. (In other words, prove that $F_3$, $F_6$, $F_9$ and so on are all even.)
**P17** Prove that

$$F_n F_{n+2} + (-1)^n = F_{n+1}^2$$

for all positive integers $n$.

## 2.7 The Euler $\varphi$ function

In general, a function defined on the positive integers (i.e. with $\mathbb{Z}^+$ as the domain) is usually called an *arithmetic function*. There are many interesting and useful arithmetic functions, but in this course we shall only have time to look at one.

**Definition 16.** For any positive integer $n$, we define $\varphi(n)$ to be the number of elements in the set $\{1, 2, \ldots, n\}$ that are coprime to $n$.

**Example 32.** Among the numbers 1, 2, 3, 4, only the number 1 and 3 are coprime to 4. Hence $\varphi(4) = 2$.

**Example 33.** Among the numbers 1, 2, 3, 4, 5, 6, 7, every number except 7 is coprime to 7. Hence $\varphi(7) = 6$.

**Theorem 24.** If the prime factorization of $n$ is $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then the following formula holds:

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

*Proof.* Omitted. □

We will not need the above general formula (and you don't have to remember it for the exam), but we shall need the following two special cases (which you must remember).

**Corollary 1.** If $p$ is a prime number, then $\varphi(p) = p - 1$. If $p$ and $q$ are different prime numbers, and $n = pq$, then $\varphi(n) = (p-1)(q-1)$.

*Proof.* This follows from the general formula. □

**Example 34.** Using the corollary, we can compute that

$$\begin{aligned} \varphi(11) &= 10 \\ \varphi(29) &= 28 \\ \varphi(15) &= 2 \cdot 4 = 8 \\ \varphi(35) &= 24 \\ \varphi(22) &= 10 \end{aligned}$$

**Theorem 25** (Euler's theorem)**.** Let $n \geq 2$ be an integer, and let $a$ be a positive integer coprime to $n$. Then the following congruence holds:

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

*Proof.* This will be proved later, using a general theorem in group theory. □

**Theorem 26** (Fermat's little theorem)**.** If $p$ is a prime number, and $a$ is a positive integer, then

$$a^p \equiv a \pmod{p}$$

*Proof.* We consider two cases.
**Case 1: $p$ divides $a$.**
In this case, $a \equiv 0 \pmod{p}$. Hence $a^p \equiv 0 \pmod{p}$, so the theorem is true in this case.
**Case 2: $p$ does not divide $a$.**
We know that $\phi(p) = p - 1$. Since $a$ is coprime to $p$, we may apply Euler's theorem (with $n = p$) to get the following congruence:

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

Multiplying both sides by $a$ proves the theorem also in the second case. □

**Example 35.** These two theorems are of great help when dealing with congruences mod a prime number. Consider for example the following question:

> What is the remainder of $4^{22}$ when divided by 7?

Since $4^{22}$ is a very large number, the question looks difficult. But Fermat's little theorem tells us that

$$4^7 \equiv 4 \pmod{7}$$

Raising both sides to the power 3 gives us

$$4^{21} \equiv 4^3 \pmod 7$$

and multiplying both sides by 4 gives

$$4^{22} \equiv 4^4 \pmod 7$$

Since $4^4 = 256$, and the number 256 gives remainder 4 when divided by 7, we can conclude that $4^{22}$ also gives remainder 4.

### 2.7.1 Exercises

Compute the following, using either the definition of $\varphi$ or the general formulae:
**E181** $\varphi(16)$
**E182** $\varphi(77)$
**E183** $\varphi(12)$
**E184** $\varphi(21)$
**E185** $\varphi(39)$
**E186** $\varphi(19)$
**E187** Prove that $2^{62} \equiv 4 \pmod{77}$.
**E188** Prove that $8^{25} \equiv 8 \pmod{39}$.
**E189** Prove that $(5^{21} - 125)$ is a multiple of 19.
**E190** Prove that if $p$ is a prime number, then

$$a^{p^2} \equiv a \pmod p$$

for every positive integer $a$.
**E191** Find the remainder when $6^{89}$ is divided by 11.
**E192** Find the last digit of the integer $7^{401}$.
**E193** Find the remainder when $3 \cdot (5^{56})$ is divided by 8.

### 2.7.2 Problems

**P18** Let $a$ and $b$ be positive integers, and let $p$ be a prime number. Prove that

$$(a+b)^p \equiv a^p + b^p \pmod p$$

**P19** Let $p$ be an odd prime number. Prove that the sum

$$1^p + 2^p + \ldots + (p-1)^p$$

is divisible by $p$.

## 2.8 Arithmetic mod n

For any integer $n \geq 2$, we introduce the set

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

For example, $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. The elements of $\mathbb{Z}_n$ can be added, subtracted and multiplied according to the following rule (we say that the arithmetic operations are performed mod $n$):

> Perform the operation (addition, subtraction or multiplication) in the usual way to get some number $M$, and then replace $M$ by the unique element of $\mathbb{Z}_n$ that is congruent to $M$ mod $n$.

The set $\mathbb{Z}_n$ is an example of an algebraic structure called a *ring*.

**Example 36.** In the ring $\mathbb{Z}_6$, the following is true:

$$\begin{aligned} 2+3 &= 5 \\ 3+4 &= 1 \\ 5+5 &= 4 \\ 3-4 &= 5 \\ 0-4 &= 2 \\ 5-1 &= 4 \\ 4 \cdot 2 &= 2 \\ 2 \cdot 3 &= 0 \\ 3 \cdot 3 &= 3 \\ 5 \cdot 5 &= 1 \end{aligned}$$

**Example 37.** In the ring $\mathbb{Z}_{13}$, the following is true:

$$\begin{aligned} 8+7 &= 2 \\ 1+12 &= 0 \\ 4-6 &= 11 \\ 1-12 &= 2 \\ 5 \cdot 8 &= 1 \\ 4 \cdot 2 &= 8 \\ 2 \cdot 11 &= 9 \end{aligned}$$

For any integer $n \geq 2$, we also introduce the set

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid k \text{ is coprime to } n\}$$

Examples:

$$\begin{aligned}
\mathbb{Z}_4^* &= \{1,3\} \\
\mathbb{Z}_6^* &= \{1,5\} \\
\mathbb{Z}_{11}^* &= \{1,2,3,4,5,6,7,8,9,10\} \\
\mathbb{Z}_8^* &= \{1,3,5,7\} \\
\mathbb{Z}_9^* &= \{1,2,4,5,7,8\}
\end{aligned}$$

Note that the number of elements in $\mathbb{Z}_n^*$ is equal to $\varphi(n)$. The elements of $\mathbb{Z}_n^*$ can be multiplied, by the same rule as above. However, if you try to add or subtract, it will not work, because you sometimes will get a result that is not in $\mathbb{Z}_n^*$. For example, $2+4$ doesn't make sense in $\mathbb{Z}_9^*$. The set $\mathbb{Z}_n^*$ is an example of a *group*.

**Example 38.** In the group $\mathbb{Z}_9^*$, the following is true:

$$\begin{aligned}
5 \cdot 2 &= 1 \\
4 \cdot 8 &= 5 \\
2 \cdot 2 &= 4
\end{aligned}$$

**Example 39.** In the group $\mathbb{Z}_8^*$, the following is true:

$$\begin{aligned}
1 \cdot 5 &= 5 \\
3 \cdot 3 &= 1 \\
5 \cdot 5 &= 1 \\
7 \cdot 7 &= 1 \\
5 \cdot 7 &= 3
\end{aligned}$$

We make the following definition:

**Definition 17.** Let $x$ be an element of the group $\mathbb{Z}_n^*$. We define the *order* of $x$ to be the smallest positive integer $k$ with the property that $x^k = 1$.

**Example 40.** We compute the order of 2 in the group $\mathbb{Z}_9^*$.

$$\begin{aligned}
2^2 &= 4 \\
2^3 &= 8 \\
2^4 &= 7 \\
2^5 &= 5 \\
2^6 &= 1
\end{aligned}$$

so the order of 2 is 6.

**Example 41.** We compute the order of 4 in the group $\mathbb{Z}_5^*$.

$$4^2 = 1$$

so the order of 4 is 2.

**Example 42.** In any group $\mathbb{Z}_n^*$, the order of 1 is 1.

**Example 43.** From the calculations in Example 39 above, we see that every element in $\mathbb{Z}_8^*$ (except the element 1) has order 2.

In the ring $\mathbb{Z}_n$ we can solve equations, just as we usually do with ordinary numbers. The general way of solving any such equation is to check *all* possible values of $x$, to see which ones satisfy the equation.

**Example 44.** Solve the equation

$$x + 6 = 2$$

in the ring $\mathbb{Z}_8$.
Solution: $x = 4$. This can be seen either by adding 2 to both sides of the equation, or by trying all possible values of $x$ (that is 0, 1, 2, 3, 4, 5, 6, 7) to see that 4 is the only solution.

**Example 45.** Solve the equation

$$3x + 5 = 1$$

in the ring $\mathbb{Z}_5$.
Solution: Try all possible values of $x$. You will find that the only solution is $x = 2$.

**Example 46.** Solve the equation

$$x^2 = 1$$

in the ring $\mathbb{Z}_8$.
Solution: Try all possible values of $x$. You will find that there are four solutions: $x = 1$, $x = 3$, $x = 5$ and $x = 7$.

**Example 47.** Solve the equation

$$x^2 = 3$$

in the ring $\mathbb{Z}_7$.
Solution: Try all possible values. You will see that there are no solutions.

### 2.8.1 Exercises

Compute in the ring $\mathbb{Z}_{12}$
**E194** $3 \cdot 7$
**E195** $3 \cdot 8$
**E196** $2 \cdot 7$
**E197** $5 \cdot 5$
**E198** $10 \cdot 1$
**E199** $3 + 11$
**E200** $3 - 11$
**E201** $0 - 1$
**E202** $6 + 7$
Compute in the ring $\mathbb{Z}_5$
**E203** $3 \cdot 2$
**E204** $4 - 4$
**E205** $1 - 4$
**E206** $4 \cdot 4$
Solve the following equations in the ring $\mathbb{Z}_9$
**E207** $x - 6 = 7$
**E208** $8x - 3 = 2$
**E209** $x^2 + 3 = 1$
**E210** $x^2 = 0$
Solve the following equations in the ring $\mathbb{Z}_5$
**E211** $x^2 = 1$
**E212** $x - 3 = 2$
**E213** $x^2 = 3$
**E214** $x^2 + x = 0$
**E215** $x^3 = 2$
**E216** Compute the order of 5 in the group $\mathbb{Z}_7$.
**E217** Compute the order of 2 in the group $\mathbb{Z}_{11}$.
**E218** Compute the order of 14 in the group $\mathbb{Z}_{15}$.

### 2.8.2 Problems

**P20** Consider the function

$$\begin{aligned} f : \mathbb{Z}_5 &\to \mathbb{Z}_5 \\ x &\mapsto 4x \end{aligned}$$

Is $f$ injective? Is $f$ surjective? Is $f$ bijective?
**P21** Consider the function

$$\begin{aligned} g : \mathbb{Z}_{10} &\to \mathbb{Z}_{10} \\ x &\mapsto 4x \end{aligned}$$

Is $g$ injective? Is $g$ surjective? Is $g$ bijective?

## 2.9 Answers and solutions

### 2.9.1 Exercises

**E155** False. **E156** False. **E157** True. **E158** True. **E159** False. **E160** False. **E161** True. (If $n$ is even, then $n = 2k$ for some $k$, and if $n$ is odd, then $n = 2k - 1$ for some $k$.) **E162** False. (It should be $n^3 \equiv 2 \pmod 5$.) **E163** True. (Since $8|16$ and $16|(a - b)$, we can conclude that $8|(a - b)$.) **E164** False. (For example, 1 is congruent to 6 mod 5, but not mod 10.) **E165** True. (Multiply both sides by (-1).) **E166** True. (Add 4 to both sides.) **E167** False. (You cannot raise one side to 2 and the other side to 3.) **E168** False. (You cannot cancel 2 from both sides, because 2 is not coprime to 4.) **E169** True. (Because 3 is coprime to 7.) **E170** 0 and 1. **E171** 0, 1 and 4. **E172** Yes, because $GCD(2, 3)$ divides 7. One solution is $x = 2$, but there are many other solutions also. **E173** No, because $GCD(8, 12)$ does not divide 6. **E174** No, because $GCD(9, 6)$ does not divide 2. **E175** Yes, because $GCD(3, 8)$ divides 5. One solution is $x = 7$, but there are many other solutions also. **E176** Yes, by the Chinese Remainder Theorem. One solution is 17. **E177** Yes, by the Chinese Remainder Theorem. One solution is 71. (The positive integers congruent to 8 mod 9 are the numbers 8, 17, 26, 35, 44 and so on. Check each number in this list until you find one that gives remainder 1 when divided by 10.) **E178** Here we cannot apply the Chinese Remainder Theorem, because 4 and 6 are not coprime. If such a number existed it would have to be both even and odd, which is of course impossible. So the answer is no.
**E179** Base step: $S(1)$ is the statement $1 \equiv 8 \pmod 7$, which is true.
Induction step: We assume that

$$2^{3n} \equiv 1 \pmod 7$$

Multiply both sides by $2^3$. This gives

$$2^{3(n+1)} \equiv 8 \pmod 7$$

and since $8 \equiv 1 \pmod 7$, this completes the induction step.
**E180** Base step: $S(1)$ is the statement $3 \equiv 3 \pmod 6$, which is true.
Induction step: We assume that

$$3^n \equiv 3 \pmod 6$$

Multiply both sides by 3. We get

$$3^{n+1} \equiv 9 \pmod 6$$

and since $9 \equiv 3 \pmod 6$, we have proved the statement $S(n + 1)$.
**E181** 8. **E182** 60. **E183** 4. **E184** 12. **E185** 24. **E186** 18.

**E187** Euler's theorem (with $n = 77$ and $a = 2$) says that

$$2^{60} \equiv 1 \pmod{77}$$

Multiply both sides by 4.
**E188** Euler's theorem (with $n = 39$ and $a = 8$) says that

$$8^{24} \equiv 1 \pmod{39}$$

Multiply both sides by 8.
**E189** Euler's theorem (with $n = 19$ and $a = 5$) says that

$$5^{18} \equiv 1 \pmod{19}$$

Multiply both sides by 125. This gives

$$5^{21} \equiv 125 \pmod{19}$$

in other words, $(5^{21} - 125)$ is a multiple of 19.
**E190** Fermat's little theorem says

$$a^p \equiv a \pmod{p}$$

Raising both sides to $p$ gives

$$a^{p^2} \equiv a^p \pmod{p}$$

and combining these two congruences shows the desired result.
**E191** Euler's theorem (with $n = 11$ and $a = 6$) says that

$$6^{10} \equiv 1 \pmod{11}$$

Raise both sides to 9 to get

$$6^{90} \equiv 1 \pmod{11}$$

Since $1 \equiv 12 \pmod{11}$, we also have

$$6^{90} \equiv 12 \pmod{11}$$

Since 6 is coprime to 11, we may cancel 6 on both sides. This gives

$$6^{89} \equiv 2 \pmod{11}$$

so the answer is 2.
**E192** The last digit is the same thing as the remainder when divided by 10.
Euler's theorem (with $n = 10$ and $a = 7$) says that

$$7^4 \equiv 1 \pmod{10}$$

Raise both sides to 100. We get

$$7^{400} \equiv 1 \pmod{10}$$

Multiply both sides by 7. We see that the answer is 7.
**E193** Euler's theorem (with $n = 8$ and $a = 5$) says that

$$5^4 \equiv 1 \pmod{8}$$

Raise both sides to 14. This gives

$$5^{56} \equiv 1 \pmod{8}$$

Now multiply both sides by 3. We get

$$3 \cdot 5^{56} \equiv 3 \pmod{8}$$

so the answer is 3.
**E194** 9. **E195** 0. **E196** 2. **E197** 1. **E198** 10. **E199** 2. **E200** 4. **E201** 11. **E202** 1. **E203** 1. **E204** 0. **E205** 2. **E206** 1. **E207** $x = 4$. **E208** $x = 4$. **E209** $x = 4$ and $x = 5$. **E210** $x = 0$, $x = 3$ and $x = 6$. **E211** $x = 1$ and $x = 4$. **E212** $x = 0$. **E213** No solutions. **E214** $x = 0$ and $x = 4$. **E215** $x = 3$. **E216** 6. **E217** 10. **E218** 2.

### 2.9.2 Problems

**P10** Try small prime numbers first.

| $p$ | $p^2+2$ |
|---|---|
| 2 | 6 |
| 3 | 11 |
| 5 | 27 |
| 7 | 51 |
| 11 | 123 |

Among the primes in this table, only the prime 3 has the property that $(p^2+2)$ is also a prime. We try to prove that no other primes has this property. The only thing we have learnt about primes in this section is Theorem 20. We have checked the primes 2 and 3 in the table, so we can assume $p \geq 5$, and we only have to consider the two cases of congruence mod 6 in the theorem.

**Case 1:** $p \equiv 1 \pmod 6$. Raising both sides to 2 gives

$$p^2 \equiv 1 \pmod 6$$

Adding 2 to both sides gives

$$p^2 + 2 \equiv 3 \pmod 6$$

so $p^2+2$ must be divisible by 3, and hence it is not a prime.

**Case 2:** $p \equiv 5 \pmod 6$. Exactly the same argument shows that $(p^2+2)$ is again divisible by 3, so it is not a prime.

Hence 3 is the only prime such that $(p^2+2)$ is also prime.

**P11** Just as in the case treated in the text, we can write

$$n = \sum_{j=0}^{k} a_j \cdot 10^j$$

The alternating digit sum is

$$\sum_{j=0}^{k} (-1)^j a_j = a_0 - a_1 + a_2 - \ldots$$

If $j$ is even, then

$$a_j \equiv a_j \cdot 10^j \pmod{11}$$

and if $n$ is odd, we have

$$-a_j \equiv a_j \cdot 10^j \pmod{11}$$

Adding these congruences for all $j$ shows that $n$ is congruent to its alternating digit sum, mod 11.

**P12** We use Theorem 20.
**Case 1:** $p$ gives remainder 1 when divided by 6.
In this case we have

$$p = 6q + 1$$

where $q$ is the quotient on division by 6. This implies

$$p^2 - 1 = 36q^2 + 12q = 12q(3q + 1)$$

If $q$ is even, then clearly $12q$ is divisible by 24, so $(p^2 - 1)$ is also divisible by 24. If $q$ is odd, then $(3q + 1)$ is even, so $12(3q + 1)$ is divisible by 24. Hence $(p^2 - 1)$ is divisible by 24 also in this case.
**Case 2:** $p$ gives remainder 5 when divided by 6.
Now we can write

$$p = 6q + 5$$

and use a similar argument as in Case 1.
**P13** Since we always have the congruence

$$38x \equiv 4x \pmod{17}$$

the Problem is the same as finding a solution to

$$4x \equiv 5 \pmod{17}$$

The positive integers congruent to 5 mod 17 are:

$$5, 22, 39, 56 \ldots$$

Since $56 = 4 \cdot 14$, we can take $x = 14$.
**P14** Suppose there exists such a positive integer $n$. Let

$$m = n^2 - n$$

The condition in the problem is the same as saying that every prime number $p$ divides $m$. This can happen only if $m = 0$, that is, only if $n = 1$. Hence $n = 1$ is the only positive integer with the given property.
**P15** We try to find a pattern.

$$\begin{aligned} 1 &= 1 \\ 1 + 3 &= 4 \\ 1 + 3 + 5 &= 9 \\ 1 + 3 + 5 + 7 &= 16 \\ 1 + 3 + 5 + 7 + 9 &= 25 \end{aligned}$$

It seems like the sum of the first $n$ odd numbers is equal to $n^2$, and we guess that this is always true. The $k$th odd number is $(2k - 1)$, so our guess says that

$$\sum_{k=1}^{n} (2k - 1) = n^2$$

We could prove it by induction, as before, but here we give an alternative solution, using Theorem 22, which we have already proved.
We compute, using basic properties of summation:

$$\begin{aligned}\sum_{k=1}^{n}(2k-1) &= 2\cdot\sum_{k=1}^{n}k-\sum_{k=1}^{n}1\\ &= 2\cdot\frac{n(n+1)}{2}-n\\ &= n^2+n-n\\ &= n^2\end{aligned}$$

which proves our guess.
**P16** We let $S(n)$ be the statement

"$F_{3n}$ is even"

**Base step:** Since $F_3 = 2$, the statement $S(1)$ is true.
**Induction step:** We assume that $S(n)$ is true, in other words that $F_{3n}$ is even. We have

$$\begin{aligned}F_{3n+1} &= F_{3n}+F_{3n-1}\\ F_{3n+2} &= F_{3n+1}+F_{3n}=2F_{3n}+F_{3n-1}\\ F_{3n+3} &= F_{3n+2}+F_{3n+1}=3F_{3n}+2F_{3n-1}\end{aligned}$$

(The second line is obtained using the definition of $F_{3n+1}$, and the last equality is obtained by adding the first two equations.) Beacuse $F_{3n}$ is even, and $2F_{3n-1}$ is even, we can conclude that

$$3F_{3n}+2F_{3n-1}$$

also is even. In other words, $S(n+1)$ is true. This completes the induction proof.
**P17** We let $S(n)$ be the formula to be proved.
**Base step:** Since $F_1 = 1$, $F_2 = 1$, and $F_3 = 2$, the statement $S(1)$ is true.
**Induction step:** We assume that $S(n)$ is true, in other words that

$$F_nF_{n+2}+(-1)^n = F_{n+1}^2$$

We add $[(-1)^{n+1}+F_{n+1}F_{n+2}]$ to both sides. This gives

$$F_nF_{n+2}+F_{n+1}F_{n+2} = F_{n+1}^2+F_{n+1}F_{n+2}+(-1)^{n+1}$$

(Here we have used that $(-1)^n+(-1)^{n+1}=0$.)
This equation can be rewritten as

$$(F_n+F_{n+1})\cdot F_{n+2} = F_{n+1}(F_{n+1}+F_{n+2})+(-1)^{n+1}$$

and this implies

$$F_{n+2}^2 = F_{n+1}F_{n+3} + (-1)^{n+1}$$

which means that we have proved the statement $S(n+1)$. This completes the induction proof.

**P18** By Fermat's theorem, we have

$$a^p \equiv a \pmod{p}$$

and

$$b^p \equiv b \pmod{p}$$

Adding these two congruences gives

$$a^p + b^p \equiv a + b \pmod{p}$$

But Fermat's theorem also says

$$(a+b)^p \equiv a + b \pmod{p}$$

which proves the desired congruence.

**P19** We let

$$m = 1^p + 2^p + \ldots + (p-1)^p$$

By Fermat's last theorem

$$\begin{aligned} 1 &\equiv 1^p \pmod{p} \\ 2 &\equiv 2^p \pmod{p} \\ 3 &\equiv 3^p \pmod{p} \end{aligned}$$

and so on. Adding all these congruences shows that

$$1 + 2 + \ldots + (p-1) \equiv m \pmod{p}$$

By Theorem 22, we know that

$$1 + 2 + \ldots + (p-1) = \frac{p-1}{2} \cdot p$$

Since $p$ is odd, the number $\frac{p-1}{2}$ is an integer, so the above equation shows that the sum

$$1 + 2 + \ldots + (p-1)$$

is a congruent to 0 mod $p$. Hence $m$ is also congruent to 0 mod $p$.

**P20** We compute all values of $f$ and collect them in a table:

| $x$ | $f(x)$ |
|---|---|
| 0 | 0 |
| 1 | 4 |
| 2 | 3 |
| 3 | 2 |
| 4 | 1 |

From the table, it is clear that $f$ is injective and surjective. Hence it is also bijective.

**P21** We compute all values of $g$ and collect them in a table:

| $x$ | $f(x)$ |
|---|---|
| 0 | 0 |
| 1 | 4 |
| 2 | 8 |
| 3 | 2 |
| 4 | 6 |
| 5 | 0 |
| 6 | 4 |
| 7 | 8 |
| 8 | 2 |
| 9 | 6 |

Now it is clear that $g$ is NOT injective (for example, $g(0) = g(5)$). It is also clear that $g$ is NOT surjective (for example, 1 is not in the image). Therefore, $g$ is also not bijective.

# 3 Proofs

We have on several occasions in the lectures discussed various kinds of proofs. Let us summarize these discussions, and also add a few things. Hopefully this will help you to prove things in the exam, and to understand the proofs given in the course. I also hope it will help you to understand books in pure mathematics in the future.

## 3.1 Theorems

In mathematics, the word "Theorem" means "true statement". We have seen many examples in the course. Sometimes we use a different word, as we have seen on a few occasions. Here are the words that are in common use in mathematical literature. We could (as we have done almost everywhere in these notes) use the word Theorem for all true statements, but the use of different words can help us to understand the structure of a chapter or a research paper, and to know what statements are more important than others.

- **Lemma** A lemma is a "small" theorem, that we want to use to prove a more important theorem later. Usually, the lemma is not really interesting in itself. Most lemmas have very short proofs. Sometimes, one proves several lemmas, and then uses all of them to prove an important theorem.
- **Corollary** A corollary is a theorem that follows immediately from a theorem we already have proved, for example by applying the theorem to a particular situation. For example, in these notes, Bezout's theorem (Theorem 8) can be regarded as a corollary to Theorem 7 (see page 23).
- **Proposition** A proposition is a theorem that is of interest in itself, but it is still not a major, very important theorem.
- **Theorem** In many textbooks, the word Theorem is used only for statements that are of a major importance.
- **Fact** In any serious textbook in pure mathematics, any theorem/lemma/proposition/corollary should be followed by a proof. Many authors use the word Fact when they for some reason want to state a theorem without giving the proof.

## 3.2 Proofs

A proof is a correct argument that shows that a certain statement must be true. Whenever we state a theorem, we should also give a proof to justify

our claim that the statement is true.
In a proof you are free to use anything you know is true, such as

- Obvious facts
- Theorems that are already proved
- The definitions of the concepts involved in the theorem

For example, in the proof of Theorem 7, we used the obvious fact that if two positive integers divide each other, then they are equal. We also used the definition of GCD, the definition of linear combination, and the definition of generator. To prove Theorem 5, we used Theorem 6.

Suppose we have defined a concept, for example prime number, or ideal, or the Euler $\varphi$-function. To prove something about this concept, we MUST use either the definition, or something we have already proved about the concept. Just after we defined a concept we know *nothing* about that concept except the definition.

It is common practice to indicate the end of a proof either by a small square, as in these notes, or by the letters QED, which is an abbreviation of the Latin expression *quod erat demonstrandum* ("which was to be proved").

Many times in this course (including in the exam!), and also in future courses in pure mathematics, you will be asked to prove something. We shall look at a few common types of theorems, and discuss what kinds of proof can be suitable in these various situations.

## 3.3 Different kinds of theorems

It is impossible to list all kinds of theorems that occur in mathematics. And it is "even more impossible" to list all kinds of proofs. However, we can list a few of the most common kinds of theorems, and discuss some basic methods of proof.

### 3.3.1 If "hypotheses" then "conclusion"

This is perhaps the most common type of theorem. We are given some assumptions, (called the "hypothesis") and are asked to prove some consequence of the assumptions (a "conclusion"). In other words, we are asked to prove that the hypotheses implies the conclusion. For example, we have the following very simple theorem: If $n$ is an odd integer, then $n^2$ is also odd. Here the hypothesis is "$n$ is an odd integer" and the conclusion is "$n^2$ is odd". To prove a theorem of this kind, the following steps may help:
**Step 1:** Identify and write down the hypotheses. These are the assumptions

that we start with.
**Step 2:** Identify and write down the conclusion. This is what we are asked to prove.
**Step 3:** Identify and write down the definitions of the terms involved in the theorem. These definitions will probably be used in the proof.
**Step 4:** Try to think about consequences of the hypothesis. For example, if the hypothesis is that "$p$ is a prime number", then there are the following consequences:

- The only positive divisors of $p$ are 1 and $p$.
- $p$ is either equal to 2, equal to 3, congruent to 1 mod 6, or congruent to 5 mod 6.
- $\varphi(p) = p - 1$
- $a^p \equiv a \pmod{p}$ for any positive integer $a$.

**Step 5:** Try to think about theorems that seem related to the statement you are asked to prove. For example, if you are asked to prove something involving a congruence, you know about the following theorems:

- The rules for congruences (Theorems 13, 14, 15)
- The five equivalent formulations of congruence (page 28)
- Euler's theorem and Fermat's theorem
- Congruence mod $m$ is an equivalence relation
- A criterion for solvability of linear congruences (Theorem 18)
- The Chinese Remainder Theorem (Theorem 19)

Can you combine any of these theorems with the hypotheses to get somewhere?
**Step 6:** With the help of the previous points, try to find an argument which starts with the hypothesis, and from there proves that the conclusion must be true.

**Example 48.** Theorem: For every integer $n \geq 4$, we have the inequality $2^n \geq n^2$. Here the hypothesis is "$n$ is an integer greater than or equal to 4". The conclusion is "$2^n \geq n^2$".

**Example 49.** Theorem: If $a$ divides $b$ and $b$ divides $c$, then $a$ divides $c$. Here the hypothesis is "$a$ divides $b$ and $b$ divides $c$", and the conclusion is "$a$ divides $c$".

IMPORTANT: You must never start by assuming that the conclusion is true! Also, you may never use a hypothesis that is not stated in the theorem.

### 3.3.2 Statement 1 is equivalent to Statement 2

With this kind of statement, we are asked to prove that one statement is true if and only if another statement is true. For example, see Theorem 11. To do this we must

- Prove that Statement 1 implies Statement 2
- Prove that Statement 2 implies Statement 1

For each of these points, you can use the ideas above. In the first point, you treat Statement 1 as the hypothesis, and Statement 2 as the conclusion. In the second point, you reverse the roles of the statements.

## 3.4 Some general methods of proof

Not all theorems are of the forms mentioned above. There are a few general strategies that often can be used to prove things, regardless of what kind of theorem we are dealing with. Here are some examples:

### 3.4.1 Proof by cases

In many situations, it might be useful to distinguish between separate cases, and give a separate proof for each case. We have seen the following examples:

- In Theorem 7, we had to prove something about an ideal. We considered the case of the zero ideal, and the case of a nonzero ideal, and gave different proofs for the two cases.
- In Theorem 16, we wanted to prove something about odd integers. We considered the case where the integer is congruent to 1 mod 4, and the case where the integer is congruent to 3 mod 4.
- In proving Fermat's little theorem, we considered the case where $p|a$ and the case where $p \nmid a$.

In elementary number theory, it is very often useful to consider the various possible cases of remainder mod $m$, for some number $m$. For example, we could consider the cases of odd numbers and even numbers.

The method of proof by cases can be thought of as a method to gain more information than was originally given in the statement of the theorem. For example, it might be hard to prove a statement about a general integer $n$, while it is easier to prove the statement when $n$ is odd, or when $n$ is even, because in each of these cases we have some additional information about $n$, that can be used in the proof.

### 3.4.2 Proof by contradiction

The idea of this proof method is to *assume* that the theorem is *not true*, and then show that this implies some false statement (a *contradiction*). This false statement could for example be $0 = 1$, or any other statement that we *know* is false. We give one example of a proof using this method.

**Theorem 27.** There are infinitely many prime numbers.

*Proof.* To prove this, we shall assume that the theorem is not true, and arrive at a contradiction. Assume that the set of prime numbers is a finite set. Then we can list all the primes as $p_1, p_2, \ldots, p_r$. Let their product be $m$. Consider the number

$$n = p_1 p_2 \cdots p_r + 1$$

that is, the number $m + 1$. This number is clearly greater than each of the primes $p_i$, so it can not be prime. Hence it is composite. Take a prime $p$ which divides $n$. This prime also divides $m$, because $p$ is among the primes $p_1, p_2, \ldots, p_r$. Therefore, $p$ divides $n - m$, in other words $p|1$. This is clearly false, so we have obtained a contradiction. Therefore the theorem is true. □

### 3.4.3 Proof by induction

This has been explained earlier in these notes.

### 3.4.4 Some further advice

Here are some further ideas that might be helpful if you try to prove something.

- Try to find out what the theorem says in particular cases, in order to understand why it must be true in general.
- Make sure that you know the definitions of the concepts involved in the statement of the theorem.
- Can you reformulate the theorem? For example, if you are asked to prove something about divisibility or congruences, you may use all of the five equivalent statements on page 28.
- Try to find a counterexample to the theorem, that is an example which shows the theorem to be false. If the theorem is true, this will not be possible, but by trying you will develop a better understanding of why the theorem is true, and perhaps also find a proof of the theorem.
- Try to think about related theorems that you know are true - can you use any of them?

## 3.5 Exercises

Identify the hypotheses and conclusions in the following statements. (You don't have to prove the theorems.)

**E219** If $x$ and $y$ are positive real numbers, then the inequality

$$\frac{x}{y} + \frac{y}{x} \geq 2$$

holds.

**E220** For any positive integer $n$, the sum of the integers $1, 2, 3, \ldots n$ is equal to $\frac{n(n+1)}{2}$.

**E221** If $n > 2$ is an integer, then there are no positive integers $x$, $y$ and $z$, such that $x^n + y^n = z^n$.

**E222** Let $m$ be an integer. Then $m^2 + m + 1$ is an odd number.

## 3.6 Problems

Here are some theorems with proofs, but the proofs are not correct! For each proof, identify the mistake made.

**P22. Theorem:**
If $m$ is an even integer, then $m^2 + 2m$ is also even.

*Proof.* Since $m^2 + 2m$ is even and $2m$ is always even, the number $m^2$ must also be even. Therefore $m$ must be even. □

**P23. Theorem:**
For every positive integer $n$, the number $n^3 - n$ is divisible by 3.

*Proof.* We consider different possible cases of remainder when $n$ is divided by 3.

**Case 1:** $n \equiv 1 \pmod 3$.
Raising both sides of this congruence to 3, we get

$$n^3 \equiv 1 \pmod 3$$

Subtract the first congruence from the second. This gives

$$n^3 - n \equiv 0 \pmod 3$$

so the theorem is true in this case.

**Case 2:** $n \equiv 2 \pmod 3$.
Again, we raise both sides of this congruence to 3, to get

$$n^3 \equiv 8 \pmod 3$$

Subtracting the first congruence from the second gives

$$n^3 - n \equiv 6 \pmod 3$$

so the theorem is true also in this case, since $6 \equiv 0 \pmod 3$. This completes the proof. □

**P24. Theorem:**
A positive integer $n$ is a prime number if and only if the following congruence holds:

$$(n-1)! \equiv -1 \pmod{n}$$

(Recall that $k! = 1 \cdot 2 \cdot 3 \cdots k$.)

*Proof.* Suppose that the given congruence holds. We want to show that $n$ is prime. Let $d$ be a positive divisor of $n$ such that $d < n$. Then $d$ is among the numbers 1, 2, ..., $(n-1)$. Therefore $d$ divides $n$ and $d$ divides $(n-1)!$. By the congruence, $-1$ is a linear combination of $n$ and $(n-1)!$, so $d$ divides $-1$. Since $d$ is positive, $d$ must be equal to 1. This argument shows that $n$ has no positive divisors except 1 and $n$ itself. So $n$ is prime. □

**P25. Theorem:**
If $x^2 \equiv 3 \pmod{6}$, then $x \equiv 3 \pmod{6}$.

*Proof.* If $x^2 \equiv 3 \pmod{6}$, then because $3 \equiv 9 \pmod{6}$, we also have

$$x^2 \equiv 9 \pmod{6}$$

Raise both sides of this congruence to $\frac{1}{2}$. This gives

$$x \equiv 3 \pmod{6}$$

which completes the proof. □

## 3.7 Answers and solutions

**E219**
The hypothesis is

> "$x$ and $y$ are positive real numbers."

The conclusion is

> "The inequality
> $$\frac{x}{y} + \frac{y}{x} \geq 2$$
> holds."

**E220**
Hypothesis: " $n$ is a positive integer".
Conclusion:

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

**E221**
Hypothesis:

$n$ is an integer and $n > 2$.

Conclusion:

There are no positive integers $x$, $y$ and $z$, such that $x^n + y^n = z^n$

**E222**
Hypothesis:

$m$ is an integer.

Conclusion:

$m^2 + m + 1$ is odd.

**P22**
We are supposed to start with the hypothesis and from there prove the conclusion. The proof given starts with the conclusion and proves the hypothesis, which is completely wrong.
**P23**
If we prove something by cases, we must consider *all* possible cases. In the given situation, we should consider the cases of remainder 0, 1, and 2. The proof given only covers the cases of remainder 1 and 2. It would be correct if we added a proof for the case $n \equiv 0 \pmod 3$.
**P24**
This is an "if and only if" theorem. This means that we must prove two things: That Statement 1 implies Statement 2 and the other way around. The given proof proves that if the congruence holds, then $n$ is prime. There should also be a proof showing that if $n$ is prime, then the congruence holds.
**P25**
We are allowed to raise both sides of a congruence to a positive integer, but we cannot raise both sides to $\frac{1}{2}$, or take square roots. To see why, let $x = 3$. Then $x^2 \equiv 4 \pmod 5$, but it is NOT true that

$$x \equiv 2 \pmod 5$$

# 4 Application: RSA cryptography

There are many interesting applications of number theory and abstract algebra, especially in computer-related subjects. We shall look closer at one famous application to cryptography.

## 4.1 The problem of secure communication

Suppose that two persons want to communicate with each other, and they want to protect their communication from being overheard by a third party. This could for example be any of the following situations:

- I want to buy a book at the online bookshop Amazon. To do this, I send them my credit card number through the Internet, so that they can deduct the correct amount of money from my bank account. A skilled hacker can easily interrupt the communication, get hold of my credit card number, and use it to take all the money in my account.
- The American CIA agent John MacAgent has infiltrated the North Korean military, and wants to send some secret information back to his colleagues in the US. If someone can interrupt and understand his message, he will immediately be killed by the North Koreans.
- Sarah is deeply in love with Otieno, but her parents thinks she is too young to have a boyfriend. So Sarah needs to send secret messages to Otieno that her parents cannot understand, even if they manage to find one of the messages.
- The researchers at the company Amazing Machines Ltd has come up with an idea for a machine that could produce large amounts of electricity very cheaply. They want to discuss these ideas through email with some leading physicists in Japan, but if someone else manages to interrupt the email communication, they could steal the idea, and the company could lose millions of dollars.

So how can these problems be solved? How can these people communicate in a safe way? These kinds of problems are investigated in the field of cryptography.
The simplest way of solving the problem is to agree on some kind of encoding scheme. For example, Sarah and Otieno could agree that in their letters, every A means B, every B means C, every C means D etc. In this case, Otieno could for example send a letter with the message

H KNUD XNT

and Sarah would be very happy, and write back:

H KNUD XNT SNN, RVDDSHD!

If her mother found the piece of paper with these letters, she would not understand, and Sarah could probably convince her that this is just the password for her webmail.
There are many other, much more complicated, ways of encoding messages (any such method is called an encoding scheme) so that they are not easily readable to others. However, there are two possible problems with all of these methods.

- Problem 1: If the code is not complicated enough, it could easily be cracked by someone with a computer (perhaps Sarah's mother has computer programming as a hobby... scary!)
- Problem 2: Suppose that Sarah's father gets hold of the *first* letter, where they write down which encoding scheme to use! Then he would be able to understand *every* subsequent letter he can find, with catastrophic consequences!

The first problem can perhaps be solved by making the encoding complicated enough, but the second is a major problem! If for example my computer system agrees with the Amazon website on how to encode the credit card number, and someone gets hold of this information, then they will be able to read my credit card number even if it is encoded!
This problem can actually be overcome, by using something called *RSA cryptography*.

## 4.2 Factoring large numbers

One of the ideas behind the RSA cryptography is that it is very hard to factor large integers, even if you use a computer. You have learnt how to factor small numbers, but how would you find the prime factorization of an integer $n$ with 200 digits? Of course, you could start by checking the primes $2, 3, 5, 7$ and so on, to see if any of them divides the large number. However, such a number is so large, that you would become old and probably die before you have checked all primes up to $\sqrt{n}$, even if you used a computer. I mentioned earlier that if you can find the factorization of the number

74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359

then you would be awarded a sum of US$ 30,000. Such a prize exists to encourage research in this area, because it has an enormous impact on the millions of messages and financial transations that take place every day through the Internet and other communication channels.

## 4.3 Any message can be expressed in terms of integers

It is easy to transform any message written with letters to a message written in integers. We could use any of the common methods used in computers, such as ASCII, Unicode and so on. In this course, we will simply write 1 instead of A, 2, instead of B, and so on, up to 26 instead of Z. We will also write 0 instead of an empty space. So we could send the numbers

$$8\ 9\ 0\ 20\ 8\ 5\ 18\ 5$$

instead of the message "HI THERE".

## 4.4 The RSA Cryptosystem

Suppose that I want to be able to receive secret messages from other people. The fundamental idea is the following. I find a "one-way function", call it $E$, such that everyone can compute $E$, but only I can compute the inverse of $E$. Then anyone can send me a secret message $x$, by computing $E(x)$, and sending this value to me. Since I am the only one who can compute the inverse of $E$, I and no-one else can retrieve $x$.

### 4.4.1 Creating a one-way function

This is how I create a one-way function $E$.

1. I pick two large primes $p$ and $q$, and I put $n = pq$.
2. I compute $\varphi(n) = (p-1)(q-1)$
3. I choose an integer $e$ which is coprime to $\phi(n)$, and which satisfies $1 < e < \phi(n)$.
4. I find an integer $d$ such that $ed \equiv 1 \pmod{\varphi(n)}$
5. I define a function by
$$\begin{aligned} E : \mathbb{Z}_n &\to \mathbb{Z}_n \\ x &\mapsto x^e \end{aligned}$$
6. I make the numbers $n$ and $e$ available to everyone, so that anyone can compute $E$.

As we will prove, the inverse of $E$ is the function $x \mapsto x^d$, so I can easily compute the inverse, since I know $d$. Although everyone knows the number $n$ and the number $e$, note the following:

- It is HARD for anyone else to factor $n$, i.e. to find $p$ and $q$.

- It is HARD for anyone else to compute $\varphi(n)$, since they don't know the factorization of $n$.
- It is IMPOSSIBLE for anyone to find $d$, unless they know $\varphi(n)$.

In these points, the word HARD means that it takes an enormous amount of time - so in practice it is impossible. Of course, we assume that $p$ and $q$ are very large, otherwise it would be easy to factor $n$, and anyone could find $d$.

**Theorem 28.** The inverse of $E$ is the function $x \mapsto x^d$.

*Proof.* We must prove that $x^{ed} \equiv x \pmod{n}$, in other words, that $n$ divides $(x^{ed} - x)$. Since $n = pq$, it is enough to show that $p$ and $q$ both divide $(x^{ed} - x)$. Consider first the case of $p$. If $p$ divides $x$, then clearly $p$ also divides $(x^{ed} - x)$. If $p$ does not divide $x$, then Euler's theorem says

$$x^{p-1} \equiv 1 \pmod{p} \tag{2}$$

Since $(p-1)$ divides $\varphi(n)$, and $\varphi(n)$ divides $(ed-1)$, we see that $(p-1)$ divides $(ed-1)$. In other words, there is an integer $b$ such that

$$b(p-1) = ed - 1$$

Raise both sides of the congruence (2) to $b$. We get

$$x^{ed-1} \equiv 1 \pmod{p}$$

and multiplying both sides by $x$ gives the desired congruence. We can use exactly the same argument for $q$, and conclude that $x^{ed} \equiv x \pmod{n}$. □

### 4.4.2 How someone sends me a message

Suppose that Arnold Schwarzenegger wants to send me a message. He writes the message as a sequence of integers $m_1, m_2, \ldots$ as explained above. He then computes the numbers $E(m_1), E(m_2), \ldots$ and sends these numbers to me. Even if someone interrupts the message, he can not compute the integers $m_i$, because he does not know the number $d$.

### 4.4.3 How I decrypt a message I receive

I receive the numbers $E(m_1), E(m_2), \ldots$ from Arnold. I can then compute

$$\begin{aligned} m_1 &= E(m_1)^d \\ m_2 &= E(m_2)^d \end{aligned}$$

and so on. Then I translate these numbers into letters, and reads the message.

### 4.5 An example

Let us take an example. First I create a one-way function $E$.

1. I choose the primes $p = 23$ and $q = 11$. Of course, these are far to small to give an effective encryption for real life applications, but it will provide us with an example that is easy to follow. We get $n = 253$
2. I compute $\varphi(253) = 22 \cdot 10 = 220$
3. I must choose an integer $e$ which is coprime to 220, and which satisfies $1 < e < 220$. I choose $e = 13$
4. I find an integer $d$ such that $13d \equiv 1 \pmod{220}$. I can take $d = 17$. (See section 4.6 for more explanation on how to find $d$.)
5. I make the numbers $n = 253$ and $e = 13$ available to everyone, so that anyone can compute $E$.

If $n$ had been very large, no-one would be able to factor $n$, or find $\varphi(n)$, or find $d$.
Arnold now wants to send me the message "YEAH". He knows $n$ and $e$. The message is written as a sequence of numbers as

$$25 \quad 5 \quad 1 \quad 8$$

Arnold now computes (remember that we use arithmetic mod 253).

$$\begin{aligned} E(25) &= 25^e = 25^{13} = 27 \\ E(5) &= 15^e = 15^{13} = 136 \\ E(1) &= 1^e = 1^{13} = 1 \\ E(8) &= 8^e = 8^{13} = 248 \end{aligned}$$

and sends me the sequence

$$27 \quad 136 \quad 1 \quad 248$$

When I receive this sequence, I compute (raising each number to $d$)

$$\begin{aligned} 27^{17} &= 25 \\ 136^{17} &= 5 \\ 1^{17} &= 1 \\ 248^{17} &= 8 \end{aligned}$$

and I translate these numbers into the message "YEAH".

## 4.6 More about linear combinations

Given $e$ and $m$, how do find an integer $d$ such that $ed \equiv 1 \pmod{m}$? Well, there are several ways. You could try to put $d = 1$, then $d = 2$, then $d = 3$ and so on, and for each $d$, check whether $ed \equiv 1 \pmod{m}$, until you find a value of $d$ that satisfies this congruence. A faster way is to check the numbers $m + 1$, $2m + 1$, $3m + 1$, etc until you find a number which is divisible by $e$. Divide this number by $e$ to find $d$.

There is an even more effective (but also more complicated) method, which uses the Euclidean algorithm. To do this, we must learn how to express the integer 1 as a linear combination of two coprime integers. Knowing this, we can find integers $x$ and $y$ such that

$$1 = xe + ym$$

and then we can take $d = x$. How do we find the integers $x$ and $y$? Answer: we can actually use the Euclidean algorithm. We show two examples below to illustrate the method. The steps are as follows:

1. Go through Euclid's algorithm. Whenver you have computed $m_i$, write out the equation
$$m_{i-2} = q \cdot m_{i-1} + m_i$$
2. Work your way backwards through the steps of the Euclidean algorithm to express 1 as a linear combination $xe + ym$ of $e$ and $m$. When doing this, you use the equations
$$m_i = m_{i-2} - q \cdot m_{i-1}$$
3. Check your answer (i.e. check that $1 = xe + ym$), so that you have not made a mistake in the calculations

**Example 50.** Write 1 as a linear combination of 7 and 18.
We first go through Euclid's algorithm:

$$\begin{aligned} m_1 &= 18 \\ m_2 &= 7 \\ m_3 &= r(18, 7) = 4 \qquad \text{so } 18 = 2 \cdot 7 + 4 \\ m_4 &= r(7, 4) = 3 \qquad \text{so } 7 = 1 \cdot 4 + 3 \\ m_5 &= r(4, 3) = 1 \qquad \text{so } 4 = 1 \cdot 3 + 1 \\ m_6 &= r(3, 1) = 0 \end{aligned}$$

Now we can use these steps to express 1 as a linear combination of 7 and 18, as follows:

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (18 - 2 \cdot 7) - 7 = 2 \cdot 18 - 5 \cdot 7$$

**Example 51.** In the RSA example above, we wanted to find an integer $d$ such that

$$13d \equiv 1 \pmod{220}$$

We first express 1 as

$$1 = 13x + 220y$$

using the Euclidean algorithm:

$$\begin{aligned} m_1 &= 220 \\ m_2 &= 13 \\ m_3 &= r(220, 13) = 12 \qquad \text{so } 220 = 16 \cdot 13 + 12 \\ m_4 &= r(13, 12) = 1 \qquad \text{so } 13 = 1 \cdot 12 + 1 \\ m_5 &= r(12, 1) = 0 \end{aligned}$$

So using back-substitution we get

$$1 = 13 - 12 = 13 - (220 - 16 \cdot 13) = 17 \cdot 13 - 1 \cdot 220$$

so we can take $x = 17$, $y = -1$. As explained, we can now take $d = 17$.

## Information on the exam

In some previous year the exam was almost completely focused on group theory. This will NOT be the case this year. The questions on the exam will cover exactly the contents of these lecture notes. So if something is treated in these printed lecture notes, it can appear on the exam. However, the part on RSA cryptography (the whole of Section 4) will NOT be on the exam.

On the exam, there will be five questions. You will be asked to answer the first question (30 marks) and two of the remaining questions (20 marks each). Thus the total number of marks is 70. The first question will be fairly easy, if you have prepared properly for the exam. The other four questions will be

- Questions similar to the Problems in these notes
- Questions asking you to prove theorems that are proved in these notes.

As I said in the lectures, the last part of these notes (Group theory) will be covered after the Christmas break, in lectures by Mr James Nkuubi. This will also be on the exam.

I wish you all the best for the examinations.

# 5 Group theory

This section is an introduction to abstract algebra. This is a very useful and important subject for those of you who will continue to study pure mathematics.

## 5.1 Binary operations

### 5.1.1 Definition and examples

Throughout mathematics, we encounter the following situation: We have a set $S$, and there is a rule that combines two elements in the set to produce a new element. Let us look at a number of examples:

**Example 52.** One of the simplest and most well-known examples is perhaps the following. We consider the set $\mathbb{Z}$ and the operation of addition. Using this operation, the numbers 2 and 5 can be combined to give the number 7; the numbers 8 and 3 can be combined to give the number 11, and so on.

**Example 53.** We could also take the same set $\mathbb{Z}$, and consider the operation of multiplication, or the operation of subtraction.

**Example 54.** To take a different example, consider the set $M_{2\times 2}$ of $2 \times 2$ matrices, with real entries. Two such matrices can be multiplied to produce a new $2 \times 2$ matrix.

We make the following definition:

**Definition 18.** A *binary operation* on a set $S$ is a function from $S \times S$ to $S$.

(Recall that $S \times S$ is the set of all ordered pairs of elements of $S$.)

**Example 55.** The operation of addition is a binary operation on $\mathbb{R}$. It is also a binary operation on $\mathbb{N}$, and also on the set of complex numbers $\mathbb{C}$. It is also a binary operation on the set $P_2$ of polynomials of degree at most 2. In fact, addition is a binary operation on any vector space.

**Example 56.** The operation of multiplication is a binary operation on $\mathbb{Z}$. It is also a binary operation on $\mathbb{N}$, and on $\mathbb{R}$, and on $\mathbb{C}$.

**Example 57.** Consider the set of positive real numbers, which we denote by $\mathbb{R}^+$. The operation of division is a binary operation on this set.

**Example 58.** Let $A$ be any set, and let $S$ be the set of all functions from $A$ to $A$. Given two elements $f$ and $g$ of $S$, we can consider the composition $f \circ g$. Since this is again an element of $S$, we see that the operation of composition is a binary operation on $S$.

**Example 59.** We can define our own binary operations. For example, we can define a binary operations on the set $\mathbb{Z}$ be the formula

$$a * b = ab + 2$$

With this definition, we can compute that $4 * 3 = 14$ and $5 * (-2) = -8$.

**Example 60.** On the set $\mathbb{Z}$, we can define a binary operation by

$$a * b = \min(a, b)$$

(this means the smallest of $a$ and $b$, or if they are equal, the common value of $a$ and $b$.) We can compute

$$\begin{aligned} 5 * 2 &= 2 \\ 10 * 10 &= 10 \\ (-1) * 5 &= -1 \\ 75 * 95 &= 75 \end{aligned}$$

**Example 61.** Another possible binary operation on $\mathbb{Z}$ is the following:

$$a * b = b$$

In this case we can compute

$$\begin{aligned} 12 * 8 &= 8 \\ 10 * 10 &= 10 \\ (-1) * 5 &= 5 \\ 75 * 95 &= 95 \end{aligned}$$

**Example 62.** Define a binary operation on $\mathbb{Z}$ by

$$a * b = 3$$

We can compute

$$\begin{aligned} 5 * 2 &= 3 \\ 10 * 10 &= 3 \\ (-1) * (-8) &= 3 \\ 75 * 95 &= 3 \end{aligned}$$

**Example 63.** We can define a binary operation on the set of points in the plane $\mathbb{R}^2$ as follows: If $P$ and $Q$ are two points, we let $P * Q$ be the midpoint of the segment $PQ$.

**Example 64.** On the ring $\mathbb{Z}_n$ defined earlier in the course, we have two binary operations: multiplication mod n and addition mod n.

### 5.1.2 Examples that are NOT binary operations

There are many examples that look like binary operations but still fail to fit in the definition above. It is important that you understand the following examples, and why they are NOT binary operations[2].

**Example 65.** Consider the operation of subtraction on the set $\mathbb{N}$ of natural numbers. This is NOT a binary operation, because when you take one natural number minus another one, you don't always get a natural number. For example, $4 - 9$ is not a natural number, because it is negative.
The problem with this operation is that although it is defined for every element of $\mathbb{N} \times \mathbb{N}$, the result does not always lie in $\mathbb{N}$. Remember that a binary operation on $\mathbb{N}$ is a function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

**Example 66.** Consider the set of real numbers $\mathbb{R}$, and the operation of division. This is NOT a binary operation, because it is not defined for every ordered pair in $\mathbb{R} \times \mathbb{R}$. (You cannot divide by zero).

**Example 67.** Consider the set of all matrices with real entries (of any size). The operation of addition is NOT a binary operation on this set, because you can not always add two matrices (it only works if they are of the same size).

**Example 68.** Consider again the set $\mathbb{Z}$. If we say that "$a*b$ is some number larger than both $a$ and $b$", we have NOT defined a binary operation, because the definition is not precise. (What is the value of $5 * 4$?)

### 5.1.3 Exercises

Do the following rules define a binary operation on the set $\mathbb{Z}$?
**E223** $a * b = a - b$
**E224** $a * b = a/b$
**E225** $a * b = b^2$
**E226** $a * b = \frac{a+b}{2}$
**E227** $a * b = -1000$

### 5.1.4 Properties that binary operations can have

In order to study binary operations in a systematic way, we introduce some definitions. In each definition, we consider a binary operation $*$ on a set $S$.

**Definition 19.** The binary operation $*$ is called *commutative* if

$$a * b = b * a$$

for all $a$ and $b$ in $S$.

[2]I might have made a terrible mistake in the lecture. If I told you that $a * b = \frac{ab}{2}$ defines a binary operation on $\mathbb{Z}$, I lied to you, because this expression is not always an integer. It should be $\mathbb{R}$ instead of $\mathbb{Z}$.

**Definition 20.** The binary operation $*$ is called *associative* if

$$(a * b) * c = a * (b * c)$$

for all $a, b, c$ in $S$.

**Definition 21.** An *identity element* for the binary operation $*$ is an element $e \in S$ such that

$$a * e = a \qquad \text{and} \qquad e * a = a$$

for all $a$ in $S$.

**Definition 22.** Let $*$ be a binary operation with an identity element $e$. An *inverse* to an element $b \in S$ is an element $x \in S$ with the property that

$$b * x = e \qquad \text{and} \qquad x * b = e$$

Let us take some examples.

**Example 69.** Consider the operation $+$ on the set $\mathbb{Z}$. This operation is commutative and associative. It has an identity element, namely 0. Also, every element has an inverse: the inverse of $n$ is the number $-n$.

**Example 70.** Consider the operation of multiplication on the set $\mathbb{Z}$. This operation is commutative and associative. The operation also has an identity element, namely 1. However, every element does NOT have an inverse. In fact only the elements 1 and $-1$ have inverses. (1 is the inverse of 1, and $-1$ is the inverse of $-1$.)

**Example 71.** Consider the operation of multiplication on the set $\mathbb{R}$. It is commutative, associative and has an identity element. Every element except 0 has an inverse. (The inverse of $a$ is $\frac{1}{a}$.)

**Example 72.** Consider the operation of matrix multiplication on the set $M_{2\times 2}$. This binary operation is associative, but NOT commutative. There is an identity element (the identity matrix). Not all elements have an inverse: only the invertible matrices do.

**Example 73.** Consider the operation on $\mathbb{Z}$ given by

$$a * b = ab - 1$$

Is it associative? To check, we compute

$$a * (b * c) = a * (bc - 1) = abc - a - 1$$

and

$$(a * b) * c = (ab - 1) * c = abc - c - 1$$

so the operation is NOT associative, since these two expressions are not in general equal.
Is the operation commutative? Yes, because

$$ab - 1 = ba - 1$$

for all $a$ and $b$ in $\mathbb{Z}$.
Is there an identity element? This would be an element $e$ such that

$$ea - 1 = a$$

for all $a \in \mathbb{Z}$. This equation can be rewritten as

$$e = \frac{a+1}{a}$$

which clearly cannot be satisfied for all $a$ at once. (In fact, it cannot be satisfied at all when $a = 0$.)
Since the operation does not have an identity element, it doesn't make any sense to ask about if any element has an inverse, since the concept of inverse cannot be defined.

**Example 74.** We consider the binary operation on $\mathbb{Z}$ given by

$$a * b = \min(a, b)$$

This operation is clearly commutative. It is also associative because $(a*b)*c$ and $a*(b*c)$ are both equal to the smallest of $a$, $b$ and $c$. Does the operation have an identity element? Suppose that $e$ is an identity element. Then we would have

$$\min(a, e) = a$$

for all elements $a$. In other words, we would have $e \geq a$ for every integer $a$. Clearly there is no such integer $e$, so there is no identity element for this operation.

**Example 75.** We define a binary operation on $\mathbb{R}$ by

$$a * b = \frac{ab}{3}$$

This is clearly commutative. Is it associative? We compute

$$a * (b * c) = a * (\frac{bc}{3}) = \frac{abc}{9}$$

and

$$(a * b) * c = (\frac{ab}{3}) * c = \frac{abc}{9}$$

so the operation is associative.
Is there an identity element? This would be an element $e$ such that

$$\frac{ae}{3} = a$$

for all $a \in \mathbb{R}$. We see that $e = 3$ satisfies this condition, so 3 is an identity element.
Which elements have an inverse? An inverse to the element $a$ is an element $x$ such that

$$\frac{ax}{3} = 3$$

in other words, such that $ax = 9$. Hence every element except 0 has an inverse: the inverse of $a$ is $\frac{9}{a}$.

### 5.1.5 Closedness

**Definition 23.** Let $S$ be a set with a binary operation $*$, and let $T$ be a subset of $S$. We sat that $T$ is *closed* under the binary operation, if whenever $t_1$ and $t_2$ are in $T$, then $t_1 * t_2$ is also in $T$.

**Example 76.** Consider the set $\mathbb{R}$ with the binary operation of addition. The subset $\mathbb{Z}$ is closed under addition, because the sum of two integers is always an integer. The subset $\mathbb{Z}^+$ is also closed under addition, because the sum of two positive integers is always a positive integer. However, the subset $\mathbb{P}$ (the set of all prime numbers) is NOT closed under addition, because the sum of two primes is not always a prime.

**Example 77.** Consider the set $M_{2\times 2}$, with the binary operation of matrix multiplication. The set of invertible matrices is closed under this operation, because the product of two invertible matrices is again invertible.

### 5.1.6 Exercises

On the set $\mathbb{Z}$, we consider the binary operation $a * b = a - b$.
**E228** Is this operation commutative?
**E229** Is this operation associative?
**E230** Does the operation have an identity element?
**E231** If the operation has an identity element, which elements have an inverse?
**E232** Is the set of even integers closed under this operation?
**E233** Is the set of positive integers closed under this operation?
**E234** Is the set of prime numbers closed under this operation?
Consider the binary operation in Example 59.
**E235** Is this operation commutative?
**E236** Is this operation associative?
**E237** Does the operation have an identity element?

**E238** If the operation has an identity element, which elements have an inverse?
**E239** Is the set of even integers closed under this operation?
**E240** Is the set of positive integers closed under this operation?
**E241** Is the set of prime numbers closed under this operation?
Consider the binary operation in Example 61.
**E242** Is this operation commutative?
**E243** Is this operation associative?
**E244** Does the operation have an identity element?
**E245** If the operation has an identity element, which elements have an inverse?
**E246** Is the set of even integers closed under this operation?
**E247** Is the set of positive integers closed under this operation?
**E248** Is the set of prime numbers closed under this operation?
Consider the binary operation in Example 62.
**E249** Is this operation commutative?
**E250** Is this operation associative?
**E251** Does the operation have an identity element?
**E252** If the operation has an identity element, which elements have an inverse?
**E253** Is the set of even integers closed under this operation?
**E254** Is the set of positive integers closed under this operation?
**E255** Is the set of prime numbers closed under this operation?

### 5.1.7 Problems

Consider the binary operation in Example 63.
**P26** Is this operation commutative?
**P27** Is this operation associative?
**P28** Does the operation have an identity element?
**P29** If the operation has an identity element, which elements have an inverse?
**P30** Let $S$ be the set of points on the line $2x + y = 1$. Is this set closed under the operation?
**P31** Is the set of points with integer coordinates closed under this operation?
**P32** Is the set of points $(x, y)$ such that $x > 0$ closed under this operation?
Consider the binary operation in Example 58.
**P33** Is this operation commutative?
**P34** Is this operation associative?
**P35** Does the operation have an identity element?
**P36** If the operation has an identity element, which elements have an inverse?
**P37** Is the set of injective functions closed under this operation?

**P38** Is the set of bijective functions closed under this operation?

## 5.2 Groups: definition and examples

**Definition 24.** A set $S$ with a binary operation $*$ is called a *group* if the following conditions are satisfied:

- The operation $*$ is associative
- The operation $*$ has an identity element
- Every element of $S$ has an inverse

**Definition 25.** A group is called *abelian* if the group operation is commutative.

If the group operation is addition, we speak of an *additive* group (this can be addition of numbers, of matrices, of functions, of vectors, etc). If the group operation is some kind of multiplication, we speak of a *multiplicative* group. An additive group is always abelian (this is an unwritten agreement between all mathematicians) but a multiplicative group can be either abelian or nonabelian, depending on the situation.

### 5.2.1 Examples of groups

**Example 78.** The set $\mathbb{Z}$, with the operation of addition, is a group. Same is true for the set $\mathbb{R}$ and the set $\mathbb{C}$. However, the set $\mathbb{N}$ is NOT a group under addition, because not every element has an inverse in $\mathbb{N}$.

**Example 79.** The set $\mathbb{Z}_n$ is a group, with the operation of addition mod $n$.

**Example 80.** The set $\mathbb{Z}_n^*$ is a group, with the operation of multiplication mod $n$.

**Example 81.** Let $A$ be any set, and let $G$ be the set of bijective functions from $A$ to $A$. Then $G$ is a group under the operation of composition. If $A$ is a finite set with $n$ elements, the resulting group $G$ is called the *symmetric group* $S_n$. A bijective function from a finite set to itself is called a *permutation*. A group in which the elements are permutations is called a *permutation* group.

**Example 82.** We write $GL_2(\mathbb{R})$ for the set of all invertible $2 \times 2$ matrices with real entries. This set is a group under matrix multiplication. The letters $GL$ is an abbreviation of "general linear group".

**Example 83.** We write $SL_2(\mathbb{R})$ for the set of all $2 \times 2$ matrices with determinant equal to 1. This set is also a group under matrix multiplication. The letters $SL$ is an abbreviation of "special linear group".

**Example 84.** The last two examples are examples of so called *Lie groups* (pronounced Lee groups). These groups are very interesting objects, and the focus of much current research. We can also define $GL_n(\mathbb{R})$, as the set of all invertible $n \times n$ matrices, and $SL_n(\mathbb{R})$ as the set of all $n \times n$ matrices with determinant 1, and there are also many other similar groups of matrices, with real or complex entries.

**Example 85.** Given a geometric object, for example a cube or a rectangular card, we can study the group of *symmetries* of the object.

**Example 86.** Given any group, we can construct many new groups from it. For example, there is the center of a group, the automorphism group of a group, and the direct product of a group with itself.

### 5.2.2 Exercises

**E256** Check that the set $\mathbb{Z}$ is a group under addition.
**E257** Check that the set of positive real numbers is a group under multiplication.
**E258** Check that the set $GL_2(\mathbb{R})$ is a group under matrix multiplication.
**E259** Is the set $\mathbb{Z}$ a group under the binary operation $a * b = a + b + 1$?
**E260** Is the set $M_{2\times 2}$ a group under matrix addition?
**E261** Is the set $\mathbb{Z}$ a group under multiplication?

## 5.3 Answers and solutions

**E223** Yes. **E224** No. **E225** Yes. **E226** No. **E227** Yes.
**E228** No. **E229** No. **E230** No. There are two conditions on an identity element. The number 0 satisfies one condition but not the other. **E232** Yes.
**E233** No. **E234** No.
**E235** Yes. **E236** No. **E237** No. **E239** Yes. **E240** Yes. **E241** No.
**E242** No. **E243** Yes. **E244**. No. **E246** Yes. **E247** Yes. **E248** Yes.
**E249** Yes. **E250** Yes. **E251** No. **E253** No. **E254** Yes. **E255** Yes.
**E256** The sum of two integers is an integer, so addition is a binary operation on $\mathbb{Z}$. Addition of integers is associative. The number 0 is the identity element. The inverse of $n$ is $-n$.
**E257** The product of two positive real numbers is a positive real number, so we have a binary operation. Multiplication of real numbers is associative. The number 1 is the identity element. The inverse of $a$ is $\frac{1}{a}$.
**E258** The product of two invertible matrices is invertible, so we have a binary operation. Matrix multiplication is associative. The identity matrix is the identity element for matrix multiplication. By definition, every invertible matrix has an inverse.
**E259** Yes. The operation is associative. The identity element is $-1$. The inverse of $n$ is $(-2 - n)$.

**E260** Yes. The operation is associative. The identity element is the zero matrix, and the inverse of a matrix $A$ is the matrix $-A$.
**E261** No. The operation is associative and the number 1 is the identity element, but not every element has an inverse.
**P26** Yes. **P27** No. **P28** No.
**P30** Yes. If you take two points $P, Q$ on a line, the midpoint of $PQ$ is also on that line.
**P31** No. Take for example the points $(0, 0)$ and $(1, 1)$.
**P32** Yes.
**P33** No. **P34** Yes. **P35** Yes. **P36** The bijective functions. **P37** Yes. (See Problem 4). **P38** Yes. The composite of two bijective functions is also bijective.

## 5.4 Some basic group theory

This part of the course is covered in the lectures by Mr Nkuubi, so I refer to his lectures for the details. This part of the course will also be on the exam, although it is not in these notes! You are expected to understand the definitions and basic properties of the following concepts:

- Order of an element in a group
- Order of a group
- Homomorphism
- Isomorphism
- Kernel of a homomorphism
- Image of a homomorphism
- Subgroup
- The cyclic subgroup generated by an element
- Coset

I promised earlier in the course that I would prove Euler's theorem, using a general theorem from group theory. Let me give this proof. The general theorem is the following:

**Theorem 29** (Lagrange's theorem)**.** Let $G$ be a finite group, and let $H$ be a subgroup of $G$. Then the order of $H$ divides the order of $G$.

An immediate consequence of Lagrange's theorem is the following:

**Corollary 2.** Let $G$ be a finite group of order $g$. Let $e$ be the identity element of $G$. Then for every element $a$ of $G$, we have $a^g = e$.

*Proof.* Let $f$ be the order of the element $a$. This is also the order of the cyclic subgroup generated by $a$. By Lagrange's theorem, $f$ divides $g$, so $g = nf$ for some positive integer $n$. We have

$$a^f = e$$

by definition of $f$. Raising both sides to $n$ gives

$$a^g = e$$

which completes the proof. □

We now recall the formulation of Euler's theorem:
**Theorem:** Let $n \geq 2$ be an integer, and let $a$ be a positive integer coprime to $n$. Then the following congruence holds:

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

*Proof.* Let $r$ be the remainder when $a$ is divided by $n$. Since $a \equiv r \pmod{n}$, we also have that

$$a^{\varphi(n)} \equiv r^{\varphi(n)}$$

To prove the theorem, it is sufficient to prove that

$$r^{\varphi(n)} = 1$$

in the ring $\mathbb{Z}_n$. The number $a$ is coprime to $n$, so $r$ is also coprime to $n$. Therefore $r$ is in the group $\mathbb{Z}_n^*$. The order of this group is $\varphi(n)$, so be the Corollary above, we can conclude that

$$r^{\varphi(n)} = 1$$

in the group $\mathbb{Z}_n^*$, and hence also in the ring $\mathbb{Z}_n$. □

THE COURSE NOTES END HERE. ALL THE BEST FOR THE EXAM!