Week 1:
Introduction to Modular Arithmetic
MA180/185/190 Algebra

Angela Carnevale

Introduction to the Module

Introduction to Modular Arithmetic

Divisibility

Introduction to the module

Welcome to this module! This is the Algebra section of your 1^{st} year Mathematics module. My name is Angela and I will be your Algebra lecture this semester.

You should be registered for one of the following module codes:

- MA180
- MA185 (also register for MA186 and MA187)
- MA190

The Calculus section of this module is taught by Prof. Dane Flannery.

Note that there are several 1^{st} year Mathematics modules running in parallel. So please take a moment to check that you are in the correct lecture, and that you are registered for the correct module code(s).

This module…

…consists of two sections: Algebra and Calculus.

Algebra lectures:

- Wednesdays at 10am in AMB-1022 (Fottrell)
- Thursdays at 10am in AMB-1022 (Fottrell)

Algebra lecturer:

- Angela Carnevale (angela.carnevale@universityofgalway.ie)

Tutorials (Algebra and Calculus):

You will also have **one** tutorial per week starting next week (25 September). You should have received information regarding your tutorial timetable.

This module…

Assessment (this semester)

- 5 online homework assignments. Your best 4 out of 5 marks will be considered.
- A **final exam** in December covering both Algebra and Calculus.

You can find on the module's **Canvas page** a breakdown of how your final mark will be computed.

Slides from the Algebra lecture will be available on the external Algebra page (you can find the link on Canvas)

Syllabus

In Algebra, we will discuss **two main topics** this semester:

- **Modular arithmetic**
- **Matrix and linear algebra**

We will see theory, examples and applications of both.

Introduction to the Module

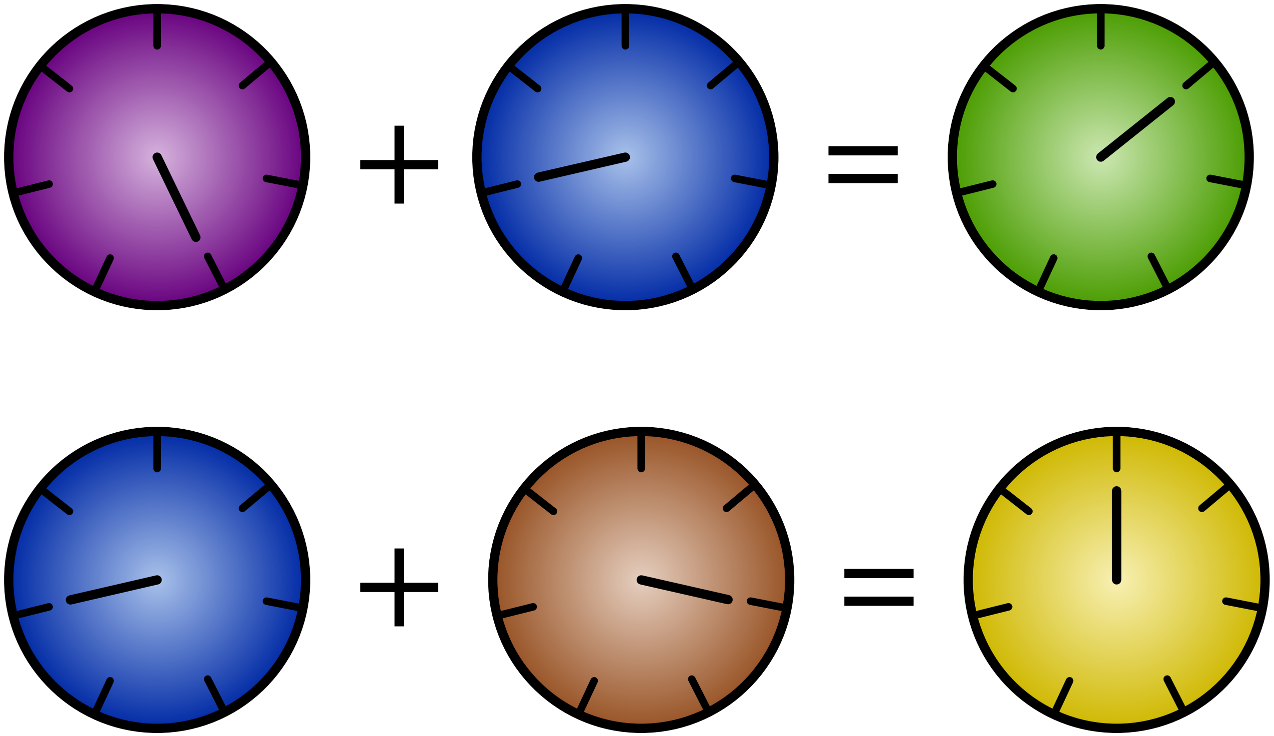
Introduction to Modular Arithmetic

Divisibility

Time

- It’s 10 o’clock. In 28 hours it will be…
- It’s Wednesday. In 16 days it will be…
- It’s September. In 14 months it will be…

Clock arithmetic



- How to define the remaining operations?
- Where is clock ("modular") arithmetic used?

Modular arithmetic in…

Modular arithmetic has numerous applications:

- Universal Product Code, IBAN, Credit Card numbers, ISBN, PPS number… Later this semester
- Cryptography Later this semester and in final year
- Transmission of Information Fields and applications

  Quantum computing…

Challenges/Problems

- There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?[1]
- We buy apples and oranges. Each apple costs 69 cents and each orange costs 35 cents. We spend €2.78. How many apples and how many oranges did we buy?
- On our credit card, one digit faded away. We can currently see:

  545762389?234113

  What's the missing digit?

These problems can all be solved with the theory we are about to build.

[1] Sunzi Suanjing, 3rd century

Numbers

Natural numbers

$\mathbb{N} = \{1, 2, 3 \ldots\}$

Integers

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3 \ldots\}$

Rational numbers

$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$

Real numbers ...

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

Divisibility

Definition

Let $a, b \in \mathbb{Z}$. We say that b **divides** a (equivalently, that b is a **divisor** of a or that b is a **factor** of a) if

$$a = b \cdot q$$

for some $q \in \mathbb{Z}$. We write $b|a$ to mean "b divides a".

Example.

- $2|10$ Indeed, $10 = 2 \cdot 5$
- $5|20$ Indeed, $20 = 5 \cdot 4$
- $3|18$ Indeed, $18 = 3 \cdot 6$
- $n|0$ for any non-zero integer n. Indeed, $0 = n \cdot 0$

Common divisors

Definition (Common divisors and gcd)

Let $a, b \in \mathbb{N}$.

- A number d such that $d|a$ and $d|b$ then d is a **common divisor** (or common factor) of a and b.
- The **largest** common divisor of a and b is called **greatest common divisor** of a and b. We use the notation $\gcd(a, b)$ for the greatest common divisor of a and b.

Example.

- 2 is a common divisor of 4 and 6. It's also the greatest common divisor, so we write $\gcd(4, 6) = 2$.

Common divisors

Definition (Common divisors and gcd)

Let $a, b \in \mathbb{N}$.

- A number d such that $d|a$ and $d|b$ then d is a **common divisor** (or common factor) of a and b.
- The **largest** common divisor of a and b is called **greatest common divisor** of a and b. We use the notation $\gcd(a, b)$ for the greatest common divisor of a and b.

Example.

- 3 is a common divisor of 12 and 18 but it's **not** the greatest common divisor.

Indeed, $6|12$ & $6|18$ and $\gcd(12,18)$

Prime numbers

Certain numbers with very few divisors hold a special place throughout mathematics (and everything else!).

Definition (prime number)

We say that a number $p \in \mathbb{N}$ with $p > 1$ is a **prime number** if its only positive divisors are 1 and p itself.