Week 2, lecture 2:
Modular arithmetic and applications

MA180/185/190 Algebra

Angela Carnevale

Introduction to Modular Arithmetic

- Modular arithmetic

Applications

- Calculus
- Credit card numbers
- PPS numbers

Congruences

We can now formalise the concept of "clock arithmetic" or **modular arithmetic**. Its foundation is the Remainder Theorem from last week. We start with the following definition.

Definition

Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$.
We say that "a is **congruent** to b **modulo** m", written

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

if $a - b$ is an integer multiple of m (equivalently, if $m|(a - b)$). The number m is called the **modulus**.

Examples.

- $9 \equiv 4 \pmod{5}$
- $29 \equiv 7 \pmod{11}$
- $69 \equiv 34 \pmod{35}$

Congruences

Note that

- $a \equiv a \pmod{m}$
- if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$
- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

Because the above properties hold, we also say that **congruence modulo** m is an **equivalence relation**[1]**.**

[1] you will see more on equivalence relations in Semester 2.

Integers modulo m and basic operations

Given a modulus m, we use the integers $\{0, 1, 2, \ldots m-1\}$ as our chosen representatives (i.e. the "hours" on the m-hour clock) to work with congruences modulo m.

We define $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$.

Example. On a 4-hour clock, we work with the numbers

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}.$$

The Remainder theorem tells us that any integer (however large or small, positive or negative) will be congruent to one of these four numbers modulo 4.

Example.

- 31 $\rightarrow$ $31-4=27$, $27-4=23$, ... $31 \equiv 3 \pmod 4$
- -23 Note: $-23+24=1$ so $-23 \equiv 1 \pmod 4$

Basic operations

Addition and multiplication modulo m are easily defined. From our definition of congruence, we have

- $a + b \equiv c \pmod{m}$ if m divides $(a + b - c)$
- $a \cdot b \equiv c \pmod{m}$ if m divides $(a \cdot b - c)$

Examples.

- $12 + 7 \equiv 3 \pmod{8}$. Indeed, $12+7-3 = 16$ which is a multiple of 8
- $7 \cdot 4 \equiv 3 \pmod{5}$. Indeed $7 \cdot 4 - 3 = 25$ which is a multiple of 5

Basic operations

Addition and multiplication modulo m are easily defined. From our definition of congruence, we have

- $a + b \equiv c \pmod{m}$ if m divides $(a + b - c)$
- $a \cdot b \equiv c \pmod{m}$ if m divides $(a \cdot b - c)$

Examples.

- $12 + 7 \equiv 3 \pmod{8}$.
- $7 \cdot 4 \equiv 3 \pmod{5}$.

When working "modulo m", we write the results of the operations as integers in the set $\mathbb{Z}_m$.

More examples

Example. • We want to compute the result of

$$-9-15 \pmod 7$$

in $\mathbb{Z}$: $-9-15=-24$

in $\mathbb{Z}_7$: $-24 \equiv 4 \mod 7$ (we added $4\cdot 7$ to "get back on the clock")

• We want to compute $6\cdot 12$ modulo 9.

$$6\cdot 12 = 72 \equiv 0 \mod 9$$

We found two non-zero numbers which give us a product of $0 \mod 9$!!!

Trigonometric functions and their values

We can use modular arithmetic to express in a compact way the angles giving certain values of sine / cosine..

Example.

$$\sin\theta = 1 \qquad \text{when } \theta = \frac{k\pi}{2} \quad \text{for } k \equiv 1 \pmod 4$$

$$\sin\theta = -1 \qquad \text{when } \theta = \frac{k\pi}{2} \quad \text{for } k \equiv 3 \pmod 4$$

...

Applications of modular arithmetic: sumchecks

Several items from our daily life have "codes" attached to them.

- When buying a product from a store, we scan its **barcode** (which contains a string made up of a number of numerical digits).
- When buying something online, we input our **credit/debit card number** for the online store to take a payment from us.
- Books have an "International Standard Book Number" (**ISBN**).
- Tax residents in Ireland have a **PPS number** (numerical digits + letters)
- …

How to avoid typos/errors in the transmission of information?

All of the codes mentioned above (and many more!) have built-in **sumchecks** to help avoid such errors. These checks are all based on modular arithmetic.

Credit card numbers

Most modern credit cards are identified by a number of parameters, including a **credit card number** made up of 16 digits between 0 and 9. The first few digits generally identify the issuer.

To avoid the transmission of incorrect information, credit card numbers satisfy the following sumcheck (also known as Luhn Algorithm)

1. Starting from the rightmost digit, add up every other digit.
2. Starting from the second digit from the right, multiply every other digit by 2. If getting a two-digit number, add those digits to get a single-digit number. Then add all the numbers found in this step.
3. Add the numbers obtained in step 1 and step 2. This number should be congruent to 0 **modulo** 10.

Modular arithmetic and credit cards

Example.

$$
\begin{array}{cccccccccccccccc}
4 & 9 & 0 & 7 & 4 & 4 & 3 & 7 & 5 & 2 & 7 & 5 & 6 & 0 & 1 & 3 \\
\times & \times & \times & \times & \times & \times & \times & \times & \times & \times & \times & \times & \times & \times & \times & \times \\
2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\
\parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\
8 & 9 & 0 & 7 & 8 & 4 & 6 & 7 & 10 & 2 & 14 & 5 & 12 & 0 & 2 & 3 \\
 & & & & & & & & \downarrow & & \downarrow & & \downarrow & & & \\
 & & & & & & & & 1 & & 5 & & 3 & & &
\end{array}
$$

here we add up the digits to get a single digit

We get $8+9+0+7+8+4+6+7+1+2+5+5+3+0+2+3 = 70 \equiv 0 \mod 10$

Back to our challenge!

Recall another of our challenges

On our credit card, one digit faded away. We can currently see:

5457 6238 9?23 4113

What's the missing digit?