## JF Maths CS1003 Hilary Term

Dr Hugh Gibbons
email: hugh.gibbons@scss.tcd.ie
Ph: 8961781 SCSS Office: 8961765

| Time\Day | **Mon.** | **Tues.** | **Wed.** |
|---|---|---|---|
| | **Lectures** | | |
| **9am** | CS1003(LB08) | | |
| **10am** | CS1003 (Joly ) | CS1003 (LB04) | |
| **3pm** | | | |
| **Tutorials** | | | |
| **12noon** | | LB08 | |
| **1pm** | | | LB04 |

# This Term (Hilary Term / $2^{nd}$ Term)

## This Term

- Set Theory
- Logic
- Number Theory

## Set Operations

$A \cup B$ is $A$ union $B$
$A \cap B$ is $A$ intersection $B$
$\overline{A}$ is the complement of $A$ i.e. the elements that are not in $A$ relative to a Universal Set.

Define a new set operator:

$$X \hat{} Y = X \cup \overline{Y}$$

Does $A\hat{}(B \cap C) = (A\hat{}B)\hat{}C$ ?

# Set Theory

A language college consists of students that study French, German or Spanish. In the college, 280 students study French, 254 students study German and 280 students study Spanish.
97 students study French as well as German,
152 students study French as well as Spanish and
138 students study German as well as Spanish.
73 students study all the three languages.

How many students are there in the language college?

# Number Sets

## Number Sets:

$\mathbb{N} = \{0, 1, 2 \dots\}$ – Natural Numbers
$\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2 \dots\}$ – Integers
$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \textit{ and } b \neq 0\}$ – Rationals (Fractions)
$\mathbb{R} = \textit{Real Numbers}$

# Set Size

Use $|S|$ for the number of elements in the set $S$
i.e. $|S|$ is the size of $S$.
Some sets have finite size, some sets are infinite.
All the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are infinite.
Since $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ , does it make sense to conclude that these sets have different sizes.
For example:
Is $|\mathbb{N}| < |\mathbb{Q}|$ since between any two natural numbers there is an infinite number of Rational numbers.?
Is $|\mathbb{N}| < |\mathbb{R}|$ since between any two natural numbers there is an infinite number of Reals?
Also, a Real number in decimal notation may have an infinite number of decimal digits
e.g. $\pi = 3.14159265358979323846264338327950288419\ldots$
**Note**: From Calculus, $\pi = 4(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} \ldots)$
**Cantor's Theorem** gives a solution to whether $|\mathbb{N}| < |\mathbb{R}|$ .

# Logic

In Logic, one can check if an argument is valid. Consider the following argument about the existence of Superman.

If Superman was able and willing to prevent evil, he would do so.
If Superman was unable to prevent evil, he would be powerless.
Superman does not prevent evil.
if Superman was unwilling to prevent evil, he would be malevolent.
If Superman exists then he is neither powerless nor malevolent.
$\therefore$(therefore)
Superman does not exist.

# Number Theory

In Computer Science, the symbol, $*$, is used for multiplication. Sometimes in Maths, the symbol $\times$ is used for multiplication and so $a * b = a \times b$. In Computer Science, $\times$ is not generally used for multiplication as $\times$ is similar to $x$.
In Maths, $ab$ can stand for $a \times b$ (e.g. $(a+b)^2 = a^2 + 2ab + b^2$) but this is not usually done in Computer Science. Instead, $(a+b)^2 = a^2 + 2 * a * b + b^2$.
Let $a, b \in \mathbb{R}$. Finding a solution, for $x$, in an equation such as $a * x = b$ is straigthforward.
It is not so straightforward when using Modular Arithmetic.
**Notation**: $(a, b, n \in \mathit{Integers})$
$a \; mod \; n$ is similar to the remainder after $a$ is divided by $n$.
e.g. "Clock Arithmetic" $23 \; mod \; 12 = 11$.
$a *_n b = (a * b) \; mod \; n$
e.g. $4 *_7 5 = (4 * 5) \; mod \; 7 = 6$.
Find an integer solution for $x$ in $3 *_7 x = 4$.
Is there a solution for $x$ in $3 *_6 x = 4$?

# Factoring into Primes

A natural number. $p$, is **prime** if it has exactly two factors, itself and 1. e.g. $2, 3, 5, 7, 11, \ldots$
The set of primes is infinite.
A natural number, $n$, is **composite** if it has a factor other than 1 and $n$. i.e. it is not prime.
A number, $n$, can be detemined composite without finding a factor.

## Fermat's Little Theorem

If, for some $a \in \mathbb{N}$, $a^n \, mod \, n \neq a \, mod \, n$ then $n$ is composite (not prime).

**Note**: $(a * b) \, mod \, n = (a \, mod \, n) \; *_n \; (b \, mod \, n)$

## Example

Let $a = 2$ and $n = 9$

$2^9 \, mod \, 9 = (2^3 *_9 2^3 *_9 2^3) = (8 *_9 8 *_9 8) = 1 *_9 8 = 8$
$(2^9 = 512$ and $512 = 9 * 56 + 8$ )
i.e. $2^9 \, mod \, 9 = 8$

Also, $2 \, mod \, 9 = 2$

$\therefore 2^9 \, mod \, 9 \neq 2 \, mod \, 9$

$\therefore$ 9 is composite.

# Corollary to Fermat's Little Theorem

## Corollary

*Let $p$ be prime and let $k$ be such that $p$ is not a factor of $k$, then $p$ is a factor of $k^{p-1} - 1$.*

## Examples

- 5 is prime and 5 is not a factor of 2 $\therefore$ 5 is a factor of $2^4 - 1$, i.e. 5 is a factor of 15.
- 5 is prime and 5 is not a factor of 8 $\therefore$ 5 is a factor of $8^4 - 1$, i.e. 5 is a factor of 4095.
- 13 is prime and 13 is not a factor of 2 $\therefore$ 13 is a factor of $2^{12} - 1$.

Check:
$2^{12} = 2^{3*4} = (2^3)^4 = 8^4 = 4096 \therefore 2^{12} - 1 = 4095$ and $4095 = 13 * 315$.

# Frank Cole 'Lecture' in 1903

Before 1876, it was not known whether $2^{67} - 1$ is prime. In 1876, Édouard Lucas proved that $2^{67} - 1$ is composite but he was unable to find its factors.

**Website**:
https://learnfunfacts.com/2017/10/09/when-frank-nelson-cole-factored-a-large-prime-during-a-lecture

At a meeting of the American Mathematics Society in 1903, Frank Cole gave a 'lecture'.
Without uttering a single word, he began to calculate the value of $2^{67} - 1$ and he got

$$147,573,952,589,676,412,927.$$

i.e.

$$2^{67} - 1 = 147,573,952,589,676,412,927$$

# Cont'd

Moving to the other side of the chalkboard, he wrote

$$193,707,721 * 761,838,257,287$$

and calculated the answer manually using long multiplication i.e.

$$193,707,721 * 761,838,257,287 = 147,573,952,589,676,412,927$$

$\therefore$

$$2^{67} - 1 = 193,707,721 * 761,838,257,287$$

$\therefore 2^{67} - 1$ is composite.

Then he got back to his seat, not having said anything during the entire 'lecture'. Despite the silence, his presentation was well-received by the audience who gave it a standing ovation.