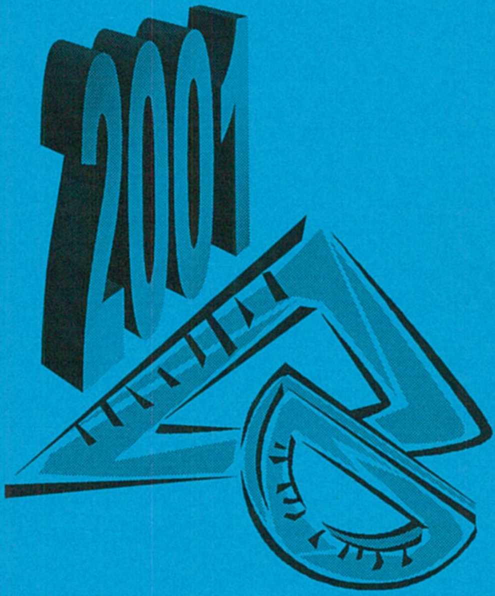
Collection III



The Collection III

Editors: I. Sciriha and A. Farrugia

Department of Mathematics

Faculty of Science

University of Malta

irene@maths.um.edu.mt
alex01@onvol.net

The Collection III

Editors: Dr. I. Sciriha and Alexander Farrugia

Department of Mathematics

Faculty of Science

University of Malta

Proceedings of Workshop held on the 27th February 2001

Contents

The Collection III

27^{th} February 2001
3.00 to 4.15pm

A workshop is being held on Tuesday, 27^{th} February 2001 from 3.00 to 4.15 p.m. to share some interesting mathematical ideas among people who find pleasure in the elegance and preciseness of mathematics.

Venue: University of Malta
Maths and Physics Building,
Department of Mathematics,
Room 316.

Speakers: Ms. Fiona Farrugia
Mr. Alex Vella and Ms. Louise Casha
Mr. Peter Borg
Mr. Alexander Farrugia
Mr. Arthur Burlo'
Mr. Vincent Mercieca

We shall end with a brief session for spontaneous problem posing and/or solving. You are cordially invited to attend.

Abstracts of possible proofs or conjectures which you wish to share with us in this meeting, or in a future one, may be sent to Dr. I. Sciriha or Ms. A. Attard, Department of Mathematics, (marked *The Collection*), at any time of the year.

Dr. I. Sciriha
(Organisor)

p.s. European Women in Mathematics 2001
10th International Meeting of **EWM**
24-30 August, 2001.
Plaza Hotel, Malta.

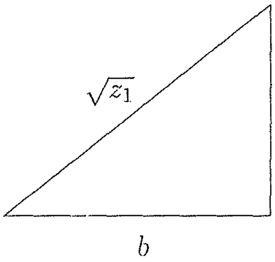
`http://www.maths.ox.ac.uk/~ewm01/`
Budding, amateur or professional mathematicians who wish to become members of the EWM may contact me.

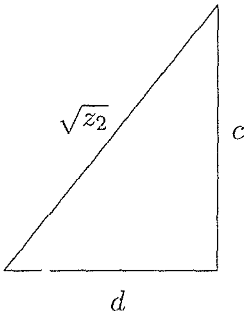
A Result in Number Theory

Fiona Farrugia

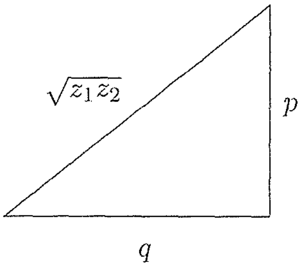
Theorem 1 *The product of 2 integers each of which is the sum of 2 squares is itself the sum of 2 squares.*

Given:





Then $\exists p, q \in \mathbb{Z}$ s.t.



Proof:

Let $z_1, z_2 \in \mathbb{Z}$ s.t. $z_1 = a^2 + b^2$ and $z_2 = c^2 + d^2$, where $a, b, c, d \in \mathbb{Z}$

We show that $\exists p, q \in \mathbb{Z}$ s.t. $z_1 z_2 = p^2 + q^2$

$\mathbb{Z}[i]$ is a Euclidean Ring with $N(a + bi) = a^2 + b^2$ and having the property: $N(g_1)N(g_2) = N(g_1 g_2)$

Let $g_1 = a + bi$ and $g_2 = c + di$ where $g_1, g_2 \in \mathbb{C}$

So $N(g_1) = a^2 + b^2$ and $N(g_2) = c^2 + d^2$

Now $g_1g_2 = (a+bi)(c+di) = (ac-bd) + i(bc+ad)$

Also $(ac-bd) \in \mathbb{Z}$ and $(bc+ad) \in \mathbb{Z}$

Let $ac-bd = p$ and $bc+ad = q$

Now $g_1g_2 \in \mathbb{Z}[i]$, hence its norm is defined.

So $N(g_1g_2) = N[(ac-bd) + i(bc+ad)] = N(p+qi) = p^2+q^2$

But we already said that $N(g_1g_2) = N(g_1)N(g_2)$

Thus $N(g_1)N(g_2) = p^2+q^2$

But $N(g_1) = a^2+b^2$ and $N(g_2) = c^2+d^2$

Thus $(a^2+b^2)(c^2+d^2) = p^2+q^2$

Hence $z_1z_2 = p^2+q^2$

Boolean Rings

Louise Casha and Alexander Vella

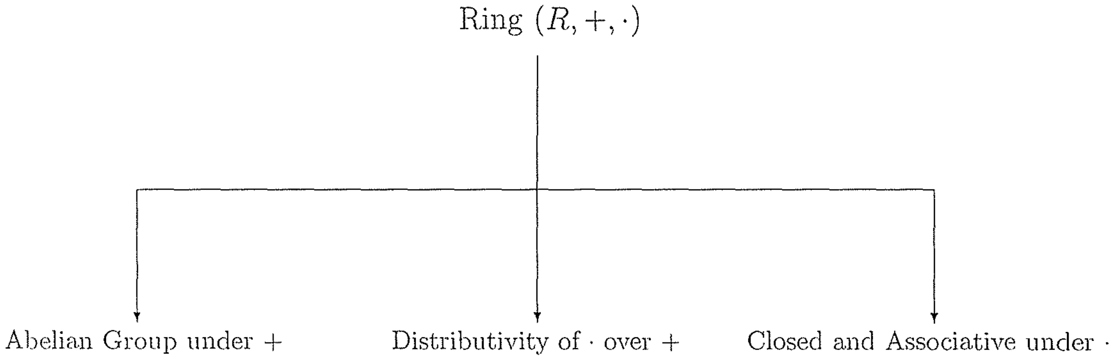

Ring $(R, +, \cdot)$
Abelian Group under $+$
Distributivity of $\cdot$ over $+$
Closed and Associative under $\cdot$

Figure 1: The definition of a Ring.

Definition of a Ring:
A *ring* is a triple comprising a set R and two binary operations $+$ and $\cdot$ satisfying the following properties (refer to Figure 1):

1. R is an Abelian group under $+$
2. R is closed and associative under $\cdot$
3. $\cdot$ is distributive over $+$

Remark: We write ab for $a \cdot b$ and x^2 for $x \cdot x$.

Definition of a Boolean Ring:
R is said to be a *Boolean Ring* if $x^2 = x \ \forall x \in R$

Theorem 1 *Let R be a Boolean Ring. Then $\forall x \in R, -x = x$*

Proof: It can be proved that if R is a ring, then $\forall a, b \in R, (-a)(-b) = ab$ and $(-x)^2 = (-x)(-x) = (x)(x) = x^2$.

$$\begin{aligned} \text{From the definition of a Boolean Ring, } x^2 &= x \\ \text{Thus } (-x)^2 &= -x \\ \text{But } (-x)^2 &= x^2 \\ \Rightarrow x &= -x, \text{ as required.} \end{aligned}$$

Theorem 2 *Let R be a Boolean Ring. Then R is commutative under $\cdot$*

Proof: Let $x, y \in R$. We need to show that $xy = yx$.

$$\begin{aligned}
(x+y)(x+y) &= (x+y) \text{ from } x^2 = x \\
x^2 + xy + yx + y^2 &= x + y \\
\text{But } x^2 = x \ &, \ y^2 = y \\
\Rightarrow x + y + xy + yx &= x + y \\
\Rightarrow xy + yx &= 0 \\
\Rightarrow yx &= -xy \\
\text{But } x &= -x \text{ from Theorem 1} \\
\text{Hence } yx &= xy, \text{ as required.}
\end{aligned}$$

Theorem 3 *Let R be a Boolean Ring. Then R is a field* $\Longleftrightarrow$ $R = \{0, 1\}$

Proof: ($\Longrightarrow$) Let R be a field and let $x \neq 0$ be in R. We need to show that $R = \{0, 1\}$.

Since R is a field, x has an inverse.
Also $x^2 = x$ since R is also a Boolean Ring.
Premultiplying both sides by x^{-1}, we get $x^{-1}x^2 = x^{-1}x \Rightarrow x = 1$

Hence if $x \neq 0$, $x = 1$. Therefore, $R = \{0, 1\}$, as required.

($\Longleftarrow$) Let $R = \{0, 1\}$. We need to show that R is a field.

It can be shown that any field has only two ideals, $\{0\}$ and itself.

Now in R the possible ideals are $\{0\}$, $\{1\}$ and $\{0, 1\}$.

- Is $\{0\}$ an ideal?

  Subgroup under + $\quad 0 \pm 0 = 0$ (closure and inverse)
  Absorption under · $\quad 0 \cdot 1 = 0$
  Hence $\{0\}$ is an ideal.

- Is $\{1\}$ an ideal?

  Absorption under · $\quad 0 \cdot 1 = 0$, hence absorption does not hold.
  Hence $\{0\}$ is NOT an ideal.

- Is $\{0, 1\}$ an ideal?

  Subgroup under + Follows since R is a ring.
  Absorption under · Follows since R is a ring.
  Hence $\{0, 1\}$ is an ideal.

Therefore, the only ideals of R are $\{0\}$ and R. Hence R is a field, as required.

The Cantor Set

Peter Borg

Consider the following sets, where C_1 is the real interval $[0,1]$ without the middle $\frac{1}{3}$ of the interval, and C_k is constructed by removing $\frac{1}{3}$ of each real interval in the union of intervals in C_{k-1}.

$$C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$$

$$C_2 = \left[0, \frac{1}{3^2}\right] \cup \left[\frac{2}{3^2}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{2}{3} + \frac{1}{3^2}\right] \cup \left[2\left(\frac{1}{3} + \frac{1}{3^2}\right), 1\right]$$

$$C_3 = \left[0, \frac{1}{3^3}\right] \cup \left[\frac{2}{3^3}, \frac{1}{3^2}\right] \cup \left[\frac{2}{3^2}, \frac{2}{3^2} + \frac{1}{3^3}\right] \cup \left[2\left(\frac{1}{3^2} + \frac{1}{3^3}\right), \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{2}{3} + \frac{1}{3^3}\right]$$
$$\cup \left[2\left(\frac{1}{3} + \frac{1}{3^3}\right), \frac{2}{3} + \frac{1}{3^2}\right] \cup \left[2\left(\frac{1}{3} + \frac{1}{3^2}\right), 2\left(\frac{1}{3} + \frac{1}{3^2}\right) + \frac{1}{3^3}\right] \cup \left[2\left(\frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3}\right), 1\right]$$

. . . etc.

It can be proved by induction on n that

$$C_n = \bigcup_{j=0}^{2^n-1} I_j$$

where

$$I_j = \left[2\sum_{i=0}^{n-1} a_i \left(\frac{1}{3}\right)^i, 2\sum_{i=0}^{n-1} a_i \left(\frac{1}{3}\right)^i + \frac{1}{3^n}\right]$$

and

$$a_i = \begin{cases} 0 \text{ if } i \bmod 2^j = 0 \\ 1 \text{ if } i \bmod 2^j = 1 \end{cases}$$

The Cantor Set is:

$$C = \lim_{n \to \infty} C_n$$

Hence, in the limit, the intervals I_j become points of the form

$$2\sum_{i=0}^{\infty} a_i \left(\frac{1}{3}\right)^i$$

where a_i is 0 or 1.

$$\text{Hence } x \in C \iff x = 2\sum_{i=0}^{\infty} a_i \left(\frac{1}{3}\right)^i, \text{ where } a_i = 0 \text{ or } 1$$

Having established which points are in the Cantor set, we can now show that these points form an uncountable set. But first we shall show that C has measure 0, and we shall do this by considering the lengths (Lesbesgue measure) of all the disjoint intervals removed from $[0,1], C_1, C_2, \ldots$ and C_{k-1} to obtain C_k, and then let $k \to \infty$. To obtain C_1 an interval of length $\frac{1}{3}$ was removed, for C_2, $2(\frac{1}{3})^2$ was removed, for C_3, $2^2(\frac{1}{3})^3$ was removed and for C_k, $2^{k-1}(\frac{1}{3})^k$ was removed. The sum of all the lengths removed is

$$2^{-1}\sum_{i=1}^{k}\left(\frac{2}{3}\right)^{i} = 1 - \left(\frac{2}{3}\right)^{k} \to 1 \text{ as } k \to \infty$$

Hence having removed a total length of 1 from $[0,1]$ we are left with a measure of 0 for C.

The binary representation for any real number in the interval $[0,1]$ is of the form

$$y = \sum_{i=1}^{\infty} a_i \left(\frac{1}{2}\right)^{i}$$

and moreover, since the real numbers in the interval in $[0,1]$ form an uncountable set and each have a binary representation, then the set B of such binary representations is uncountable.

Now if we construct the function $f : C \to B$ defined by $f(x) = y$, i.e.

$$f\left(2\sum_{i=0}^{\infty} a_i \left(\frac{1}{3}\right)^{i}\right) = \sum_{i=0}^{\infty} a_i \left(\frac{1}{2}\right)^{i}$$

we get a one-to-one and onto mapping. Therefore one can say that there are as many points in C as there are in B, which implies that the set C is uncountable.

Note:[1] The idea of defining measures using covers of sets was introduced by Carathéodory (1914). Hausdorff (1919) used this method to define the measures that now bear his name, and showed that the middle third Cantor set has positive and finite measure of dimension $\frac{\log 2}{\log 3}$.

[1] Thanks to Cettina Gauci Pulo for this information

A Problem inspired from the Cantor Set

Vincent Mercieca

Required to find a subset of $[0,1] \subseteq \mathbb{R}$ which is dense, does not contain intervals of $[0,1]$, and whose measure lies between 0 and 1.

Define

$$A_1 = \left[\frac{1}{3}, \frac{2}{3}\right]$$

$$A_2 = \left[\frac{1}{3^3}, \frac{2}{3^3}\right] \cup \left[\frac{2}{3} + \frac{1}{3^3}, \frac{2}{3} + \frac{2}{3^3}\right]$$

... etc. Then define $A = \bigcup_\infty A_i \subseteq [0,1]$.

The length of the first interval: $a_0 = 1$ The length of the second interval:

$$a_1 = \frac{1 - \frac{1}{3}}{2} = \frac{1}{3}$$

The length of the third interval:

$$a_2 = \frac{a_1 \left(1 - \left(\frac{1}{3}\right)^2\right)}{2} = \frac{\left(1 - \frac{1}{3}\right)\left(1 - \left(\frac{1}{3}\right)^2\right)}{2^2}$$

The length of the fourth interval:

$$a_3 = \frac{\left(1 - \frac{1}{3}\right)\left(1 - \left(\frac{1}{3}\right)^2\right)\left(1 - \left(\frac{1}{3}\right)^3\right)}{2^3}$$

Therefore $|A_1| = \frac{1}{3}a_0 = \frac{1}{3}, |A_2| = \frac{2}{3^2}a_1, \ldots$
Therefore $|\bigcup_\infty A_i| = \frac{1}{3}a_0 + \frac{2}{3^2}a_1 + \frac{2^2}{3^3}a_2 + \frac{2^3}{3^4}a_3 + \cdots$

Let $S_\infty = |\bigcup_\infty A_i|$, then

$$S_\infty = \frac{1}{3} + \frac{\left(1 - \frac{1}{3}\right)}{3^2} + \frac{\left(1 - \frac{1}{3}\right)\left(1 - \left(\frac{1}{3}\right)^2\right)}{3^3} + \frac{\left(1 - \frac{1}{3}\right)\left(1 - \left(\frac{1}{3}\right)^2\right)\left(1 - \left(\frac{1}{3}\right)^3\right)}{3^4} + \cdots$$

$$S_\infty = \frac{1}{3} + \frac{(3-1)}{3^3} + \frac{(3-1)(3^2-1)}{3^6} + \frac{(3-1)(3^2-1)(3^3-1)}{3^{10}} + \cdots$$

$$\cdots + \frac{(3-1)(3^2-1)\cdots(3^{n-1}-1)}{3^{\frac{n}{2}(n+1)}} + \cdots$$

$$S_\infty < \frac{1}{3} + \frac{3}{3^3} + \frac{3 \cdot 3^2}{3^6} + \frac{3 \cdot 3^2 \cdot 3^3}{3^{10}} + \cdots$$

$$\Longrightarrow S_\infty < \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \frac{1}{3^4} + \cdots$$

$$\Longrightarrow S_\infty < \frac{\frac{1}{3}}{1 - \frac{1}{3}} = \frac{\frac{1}{3}}{\frac{2}{3}} = \frac{1}{2}$$

Also $S_\infty > \frac{1}{3}$, hence $\frac{1}{3} < S_\infty < \frac{1}{2}$.

Thus if we consider all the irrational numbers in these intervals A_i, then we obtain a subset of $[0, 1]$ which is dense, contains no intervals, and its measure is between $\frac{1}{3}$ and $\frac{1}{2}$.

A Construction of the set of integers $\mathbb{Z}$

Alexander Farrugia

We'll endeavour to show the construction of $\mathbb{Z}$ from $\mathbb{N}$, the set of natural numbers. We'll then show that the set just constructed is indeed the set of integers.

To start with, we'll assume that the set of natural numbers $\mathbb{N}$ has already been constructed (set-theoretically or intuitively). Also, for uniformity's sake, we'll agree on the following set of natural numbers and integers:

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

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

i.e. we include the zero in $\mathbb{N}$. However, if we choose to omit the zero, the following construction of $\mathbb{Z}$ would still work.

Consider the set of all pairs of natural numbers, i.e. $\mathbb{N}\times\mathbb{N}$ (or $\mathbb{N}^2$). On this set, define an equivalence relation $\sim$ such that:

$$\forall\,(a,b),(c,d) \in \mathbb{N}\times\mathbb{N},\ \ (a,b) \sim (c,d) \iff a+d = b+c$$

The relation $\sim$ can be easily shown to be an equivalence relation, thus:

Reflexivity:

$$(a,b) \sim (a,b) \iff a+b = a+b, \text{ which is always true.}$$

Symmetry:

$$\begin{aligned} (a,b) \sim (c,d) &\iff a+d = b+c \\ &\iff b+c = a+d \\ &\iff (c,d) \sim (a,b) \end{aligned}$$

Transitivity:

$$\begin{aligned} (a,b) \sim (c,d) \text{ and } (c,d) \sim (e,f) &\iff a+d = b+c \text{ and } c+f = d+e \\ &\implies a+d+e = b+c+e \\ &\implies a+c+f = b+c+e \\ &\implies a+f = b+e \\ &\implies (a,b) \sim (e,f) \end{aligned}$$

Now, since $\sim$ is an equivalence relation, it induces a partition on $\mathbb{N} \times \mathbb{N}$ into equivalence classes. Here are some examples:

$$\begin{aligned}
\widehat{(0,0)} &= \{(0,0),(1,1),(2,2),\ldots\} = \{(a,a) : a \in \mathbb{N}\} \\
\widehat{(1,0)} &= \{(1,0),(2,1),(3,2),\ldots\} = \{(a+1,a) : a \in \mathbb{N}\} \\
\widehat{(0,1)} &= \{(0,1),(1,2),(2,3),\ldots\} = \{(a,a+1) : a \in \mathbb{N}\}
\end{aligned}$$

Let's introduce some notation. From now on, by $[a,b]$ we mean the equivalence class of (a,b). In other words, $[a,b] = \widehat{(a,b)}$.

Motivated by the above examples, we prove a very simple but very useful lemma:

Lemma 1 $\forall\ a,b,c \in \mathbb{N}, [a,b] = [a+c,b+c]$.

Proof:

$$\begin{aligned}
[a,b] &= \{(x,y) : x,y \in \mathbb{N} \textit{ and } a+y = b+x\} \\
&= \{(x,y) : x,y \in \mathbb{N} \textit{ and } (a+c)+y = (b+c)+x\} \\
&= [a+c,b+c]
\end{aligned}$$

as required.

Let's define $\mathbb{I}$ to be the set of all equivalence classes of $\sim$ on $\mathbb{N}\times\mathbb{N}$, i.e.

$$\mathbb{I} = \{[a,b] : a,b \in \mathbb{N}\}$$

Now seems to be the right time to make the following claim:

Claim 1 $\mathbb{I}$ *is the set of integers!*

The above claim isn't quite right yet, for we need to define addition and multiplication of any two integers in terms of the addition and multiplication of natural numbers. For this reason, from now on we distinguish between these operators by writing the addition operator as $+$ (as we were doing since we've started) and that of the integers as $\oplus$. Also, we write the product operator of the natural numbers as $\cdot$ and that of the integers as $\odot$.

Now let's define $\oplus$ and $\odot$: $([a,b],[c,d] \in \mathbb{I})$

$$[a,b] \oplus [c,d] = [a+c,b+d]$$

$$[a,b] \odot [c,d] = [ac+bd,ad+bc]$$

Immediately, however, we encounter the problem of the well-definition of the above two operators. We have already shown by the lemma that $[a,b] = [a+c,b+c]\ \forall\ a,b,c \in \mathbb{N}$ and therefore there are an infinite number of ways of writing the same equivalence class (which we claim is an integer). We need to show that however we write the two equivalence classes, we still have the same answer when added or multiplied together. That's what the following theorem does:

Theorem 1 *$\oplus$ and $\odot$ are well-defined.*

Proof:
(i) We need to show that if $[a_1, a_2] = [a_1', a_2']$ and $[b_1, b_2] = [b_1', b_2']$, then $[a_1, a_2] \oplus [b_1, b_2] = [a_1', a_2'] \oplus [b_1', b_2']$ $\forall$ $[a_1, a_2], [a_1', a_2'], [b_1, b_2], [b_1', b_2'] \in \mathbb{I}$.

$$\text{Now } [a_1, a_2] = [a_1', a_2'] \implies a_1 + a_2' = a_1' + a_2 \qquad (1)$$
$$\text{and } [b_1, b_2] = [b_1', b_2'] \implies b_1 + b_2' = b_1' + b_2 \qquad (2)$$

$$\begin{aligned}
\text{So } [a_1, a_2] \oplus [b_1, b_2] &= [a_1 + b_1, a_2 + b_2] \text{ (definition of } \oplus) \\
&= [a_1 + b_1 + a_2' + b_2', a_2 + b_2 + a_2' + b_2'] \text{ (by lemma 1)} \\
&= [a_1' + b_1' + a_2 + b_2, a_2 + b_2 + a_2' + b_2'] \text{ (from (1) and (2))} \\
&= [a_1' + b_1', a_2' + b_2'] \text{ (by lemma 1)} \\
&= [a_1', a_2'] \oplus [b_1', b_2'] \text{ (definition of } \oplus\text{), as required.}
\end{aligned}$$

(ii) We need to show that if $[a_1, a_2] = [a_1', a_2']$ and $[b_1, b_2] = [b_1', b_2']$, then $[a_1, a_2] \odot [b_1, b_2] = [a_1', a_2'] \odot [b_1', b_2']$ $\forall$ $[a_1, a_2], [a_1', a_2'], [b_1, b_2], [b_1', b_2'] \in \mathbb{I}$.

(1) and (2) from (i) still hold.

So $[a_1, a_2] \odot [b_1, b_2]$
$= [a_1b_1 + a_2b_2, a_1b_2 + a_2b_1]$ (definition of $\odot$)
$= [a_1b_1 + a_2b_2 + a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2', a_1b_2 + a_2b_1 + a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (by lemma 1)
$= [a_1(b_1 + b_2') + a_2(b_2 + b_1') + a_2'b_1' + a_1'b_2', a_1b_2 + a_2b_1 + a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (distributivity of $\mathbb{N}$)
$= [a_1(b_1' + b_2) + a_2(b_2' + b_1) + a_2'b_1' + a_1'b_2', a_1b_2 + a_2b_1 + a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (by (2))
$= [a_1b_1' + a_2b_2' + a_1b_2 + a_2b_1 + a_2'b_1' + a_1'b_2', a_1b_2 + a_2b_1 + a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (distributivity of $\mathbb{N}$)
$= [a_1b_1' + a_2b_2' + a_2'b_1' + a_1'b_2', a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (by lemma 1)
$= [b_1'(a_1 + a_2') + b_2'(a_2 + a_1'), a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (distributivity of $\mathbb{N}$)
$= [b_1'(a_1' + a_2) + b_2'(a_2' + a_1), a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (by (1))
$= [b_1'a_1' + b_1'a_2 + b_2'a_2' + b_2'a_1, a_1b_2' + a_2b_1' + a_2'b_1' + a_1'b_2']$ (distributivity of $\mathbb{N}$)
$= [a_1'b_1' + a_2'b_2', a_2'b_1' + a_1'b_2']$ (by lemma and commutativity of $\mathbb{N}$)
$= [a_1', a_2'] \odot [b_1', b_2']$ (definition of $\odot$), as required.

Now we can finally show that the set $\mathbb{I}$ is indeed the set of integers with respect to the additive and multiplicative operators $\oplus$ and $\odot$ respectively. To do this, we note that the axioms for the set of integers are only satisfied by a unique system of objects (the integers, proved in Section 3.12 in Allenby). So if our system of integers $\mathbb{I}$ satisfies all the axioms of the integers, we are done.

Note that we could have shown that $\langle \mathbb{I}, \oplus, \odot \rangle$ and $\langle \mathbb{Z}, +, \cdot \rangle$ are isomorphic (it can be easily shown), but we're assuming that $\mathbb{Z}$ does not exist (in fact we're constructing it!)

Theorem 2 $\langle \mathbb{I}, \oplus, \odot \rangle$ *is the ring of integers.*

Proof: We need to show that all the axioms for the integers are true. Let's list these axioms here:

For every three integers a, b, c we have:

$A1$ $a \oplus b = b \oplus a$
$A2$ $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
$A3$ $\exists!\ 0 \in \mathbb{I}\ s.t.\ 0 \oplus a = a \oplus 0 = a$
$A4$ $\forall a \in \mathbb{I}\ \exists! - a\ s.t.\ a \oplus (-a) = (-a) \oplus a = 0$

$M1$ $a \odot b = b \odot a$
$M2$ $(a \odot b) \odot c = a \odot (b \odot c)$
$M3$ $\exists!\ 1 \in \mathbb{I}\ s.t.\ 1 \odot a = a \odot 1 = a$

D $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ and $(a \oplus b) \odot c = a \odot c \oplus b \odot c$
P $\mathbb{I}$ contains a non-empty subset N $s.t.$
(i) $\forall a \in \mathbb{I}, a$ belongs to exactly 1 of the sets $N, \{0\}, -N$ where $-N = \{-x : x \in N\}$
(ii) $\forall a, b \in N, a \oplus b \in N$ and $a \odot b \in N$
I If $U \subseteq N$ $s.t.$ $1 \in U$ and $a \in U \Longrightarrow a \oplus 1 \in U$, then $U = N$

Let $a = [a_1, a_2], b = [b_1, b_2], c = [c_1, c_2]$.

Let's prove the above axioms one by one:

$$\begin{aligned} A1: \qquad a \oplus b &= [a_1, a_2] \oplus [b_1, b_2] \\ &= [a_1 + b_1, a_2 + b_2] \text{ (definition of } \oplus) \\ &= [b_1 + a_1, b_2 + a_2] \text{ (commutativity of } +) \\ &= [b_1, b_2] \oplus [a_1, a_2] \text{ (definition of } \oplus) \\ &= b \oplus a, \text{ as required.} \end{aligned}$$

$$\begin{aligned} A2: \qquad (a \oplus b) \oplus c &= ([a_1, a_2] \oplus [b_1, b_2]) \oplus [c_1, c_2] \\ &= [a_1 + b_1, a_2 + b_2] \oplus [c_1, c_2] \text{ (definition of } \oplus) \\ &= [(a_1 + b_1) + c_1, (a_2 + b_2) + c_2] \text{ (definition of } \oplus) \\ &= [a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)] \text{ (associativity of } +) \\ &= [a_1, b_1] \oplus [b_1 + c_1, b_2 + c_2] \text{ (definition of } \oplus) \\ &= [a_1, b_1] \oplus ([b_1, b_2] \oplus [c_1, c_2]) \text{ (definition of } \oplus) \\ &= a \oplus (b \oplus c), \text{ as required.} \end{aligned}$$

$A3$: Define $0 = [0, 0]$.
Then $[0, 0] \oplus [a_1, a_2] = [a_1, a_2] = [a_1, a_2] \oplus [0, 0]$.

Now we show that 0 is unique, i.e. if $[x_1, x_2] \oplus [a_1, a_2] = [a_1, a_2] = [a_1, a_2] \oplus [x_1, x_2]$, then $[x_1, x_2] = [0, 0]$.

$[x_1, x_2] \oplus [a_1, a_2] = [x_1 + a_1, x_2 + a_2] = [a_1, a_2]$
By lemma, $[a_1, a_2] = [a_1 + x_1, a_2 + x_1]$
$\Rightarrow x_1 = x_2$

But by the lemma again, $[x_1, x_2] = [x_1, x_1] = [0, 0] = 0$, as required.

$A4$: Define $-a = [a_2, a_1]$.

$$\begin{aligned} \text{Then } a \oplus (-a) &= [a_1, a_2] \oplus [a_2, a_1] \\ &= [a_1 + a_2, a_2 + a_1] \\ &= [0, 0] \text{ by lemma} \\ &= 0 \end{aligned}$$

By $A1$, $(-a) \oplus a = 0$

Now we show that $-a$ is unique, i.e. if $[a_1, a_2] \oplus [x_1, x_2] = [0, 0]$, then $[x_1, x_2] = [a_2, a_1]$.

$[a_1, a_2] \oplus [x_1, x_2] = [a_1 + x_1, a_2 + x_2] = [0, 0]$
By lemma, $[0, 0] = [a_1 + x_1, a_1 + x_1]$
$\Rightarrow a_1 + x_1 = a_2 + x_2 \Rightarrow x_1 + a_1 = x_2 + a_2$
For definition of $\sim$, this implies that $(x_1, x_2) \sim (a_2, a_1)$
$\Rightarrow (x_1, x_2)$ and (a_2, a_1) are in the same equivalence class
$\Rightarrow [x_1, x_2] = [a_2, a_1]$, as required.

$$\begin{aligned} M1: \qquad a \odot b &= [a_1, a_2] \odot [b_1, b_2] \\ &= [a_1 b_1 + a_2 b_2, a_1 b_2 + a_2 b_1] \text{ (definition of } \odot) \\ &= [b_1 a_1 + b_2 a_2, b_1 a_2 + b_2 a_1] \text{ (commutativity of } \cdot \text{ and } +) \\ &= [b_1, b_2] \odot [a_1, a_2] \text{ (definition of } \odot) \\ &= b \odot a, \text{ as required.} \end{aligned}$$

$$\begin{aligned} M2: \quad (a \odot b) \odot c &= ([a_1, a_2] \odot [b_1, b_2]) \odot [c_1, c_2] \\ &= [a_1 b_1 + a_2 b_2, a_1 b_2 + a_2 b_1] \odot [c_1, c_2] \text{ (definition of } \odot) \\ &= [a_1 b_1 c_1 + a_2 b_2 c_1 + a_1 b_2 c_2 + a_2 b_1 c_2, a_1 b_1 c_2 + a_2 b_2 c_2 \\ &\qquad + a_1 b_2 c_1 + a_2 b_1 c_1] \text{ (definition of } \odot) \end{aligned}$$

$$\begin{aligned}
&= [a_1(b_1c_1 + b_2c_2) + a_2(b_1c_2 + b_2c_1), a_1(b_1c_2 + b_2c_1) \\
&\qquad +a_2(b_1c_1 + b_2c_2)] \text{ (distributivity in } \mathbb{N}) \\
&= [a_1, a_2] \odot [b_1c_1 + b_2c_2, b_1c_2 + b_2c_1] \text{ (definition of } \odot) \\
&= [a_1, a_2] \odot ([b_1, b_2] \odot [c_1, c_2]) \text{ (definition of } \odot) \\
&= a \odot (b \odot c), \text{ as required.}
\end{aligned}$$

$M3$: Define $1 = [1, 0]$
Then $[1, 0] \odot [a, b] = [a, b] = [a, b] \odot [1, 0]$.

Now we show that 1 is unique, i.e. if $[x_1, x_2] \odot [a_1, a_2] = [a_1, a_2] = [a_1, a_2] \odot [x_1, x_2]$ and $a \neq 0$, then $[x_1, x_2] = [1, 0]$.

$[x_1, x_2] \odot [a_1, a_2] = [x_1a_1 + x_2a_2, x_1a_2 + x_2a_1] = [a_1, a_2]$
$\Rightarrow x_1a_1 + x_2a_2 + a_2 = x_1a_2 + x_2a_1 + a_1$, since equivalence classes are equal and by definition of $\sim$.

$$\Rightarrow x_1a_1 + a_2(x_2 + 1) = x_1a_2 + a_1(x_2 + 1) \qquad (3)$$

Let $d = [d_1, d_2], e = [e_1, e_2], d, e \neq [0, 0]$.

$[d_1, d_2] \neq [0, 0] \Rightarrow d_1 \neq d_2$ and similarly, $e_1 \neq e_2$.

$\Rightarrow d_1e_1 \neq d_1e_2, d_1e_1 \neq d_2e_1, d_2e_2 \neq d_1e_2$ and $d_2e_2 \neq d_2e_1$

$$\Rightarrow d_1e_1 + d_2e_2 \neq d_1e_2 + d_2e_1 \qquad (4)$$

Consider $[d_1, d_2] \odot [e_1, e_2] = [d_1e_1 + d_2e_2, d_1e_2 + d_2e_1] \neq [0, 0]$ by (4).

Taking the contrapositive,

$$d \odot e = 0 \Rightarrow d = 0 \text{ or } e = 0 \qquad (5)$$

Now consider $[x_1, x_2 + 1] \odot [a_1, a_2] = [x_1a_1 + (x_2 + 1)a_2, x_1a_2 + (x_2 + 1)a_1]$
From (3), this is equal to $[x_1a_1 + (x_2 + 1)a_2, x_1a_1 + (x_2 + 1)a_2] = [0, 0]$ by lemma.

From (5), either $[x_1, x_2 + 1] = [0, 0]$ or $[a_1, a_2] = [0, 0]$.

The second case is dismissed since $a \neq 0$.

Therefore, $[x_1, x_2 + 1] = [0, 0] \Rightarrow x_1 = x_2 + 1 \Rightarrow [x_1, x_2] = [1, 0]$, as required.

$$\begin{aligned}
D: \quad a \odot (b \oplus c) &= [a_1, a_2] \odot ([b_1, b_2] \oplus [c_1, c_2]) \\
&= [a_1, a_2] \odot [b_1 + c_1, b_2 + c_2] \text{ (definition of } \oplus) \\
&= [a_1(b_1 + c_1) + a_2(b_2 + c_2), a_1(b_2 + c_2) + a_2(b_1 + c_1)] \\
&\qquad \text{(definition of } \odot)
\end{aligned}$$

$$
\begin{aligned}
&= [a_1b_1 + a_1c_1 + a_2b_2 + a_2c_2, a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1]\\
&\qquad \text{(distributivity in } \mathbb{N})\\
&= [a_1b_1 + a_2b_2, a_1b_2 + a_2b_1] \oplus [a_1c_1 + a_2c_2, a_1c_2 + a_2c_1]\\
&\qquad \text{(definition of } \oplus)\\
&= [a_1, a_2] \odot [b_1, b_2] \oplus [a_1, a_2] \odot [c_1, c_2] \text{ (definition of } \odot)\\
&= a \odot b \oplus a \odot c, \text{ as required}
\end{aligned}
$$

The second case is treated similarly.

P : Define $N = \{[a, 0] : a \in \mathbb{N} \text{ and } a \neq 0\}$

(i) $\forall a = [a_1, a_2] \in \mathbb{I}$, either $a_1 = a_2$ or $a_2 < a_1$ or $a_1 < a_2$ exclusively.

$$
\begin{aligned}
\text{If } a_1 = a_2, \text{ then } a = [a_1, a_1] &= [0, 0] \text{ by lemma}\\
&= 0, \text{ so } a \in \{0\}
\end{aligned}
$$

$$
\begin{aligned}
\text{If } a_2 < a_1, \text{ then } [a_1, a_2] &= [k + a_2, a_2] \text{ where } a_1 = k + a_2\\
&= [k, 0] \text{ by lemma, so } a \in N
\end{aligned}
$$

$$
\begin{aligned}
\text{If } a_1 < a_2, \text{ then } [a_1, a_2] &= [a_1, j + a_1] \text{ where } a_2 = j + a_1\\
&= [0, j] \text{ by lemma}\\
&= -[j, 0] \text{ from } A4, \text{ so } a \in -N, \text{ as required.}
\end{aligned}
$$

(ii) Let $a, b \in N$, so that $a = [a', 0], b = [b', 0]$.
Then $[a', 0] \oplus [b', 0] = [a' + b', 0] \in N$
$[a', 0] \odot [b', 0] = [a'b', 0] \in N$, as required.

I : Let $U \subseteq N$. Then all the elements of U are of the form $[u, 0]$, where $u \in \mathbb{N}$.

$$[1, 0] \in U \tag{6}$$

$$\text{If } [u, 0] \in U \text{ then } [u, 0] \oplus [1, 0] = [u + 1, 0] \in U \tag{7}$$

Suppose

$$\exists\ [n, 0] \in N \text{ s.t. } [n, 0] \notin U \tag{8}$$

This may be possible since $U \subseteq N$

Putting $u = 1$ in (7) (as (6) tells us that $[1, 0] \in U$), we get $[2, 0] \in U$.
Applying the above and (7) $(n - 2)$ times we get $[n, 0] \in U$, which contradicts (8).

Therefore $\forall\ [n, 0] \in N, [n, 0] \in U$, which means that $N \subseteq U$

But $U \subseteq N$. Hence $U = N$, as required.

As an aside, we now revert to our usual notation for the integers. The proof of axiom P above suggests that we write $[n, 0]$ as n and $[0, n]$ as $-n$. Then we might just as well rewrite $\oplus$ as $+$ and $\odot$ as $\cdot$, so that we end up with the familiar notation for the integers!

Let's give a few examples:

$[2, 0] \oplus [3, 0] = [5, 0]$ is written as $2 + 3 = 5$
$[2, 0] \odot [3, 0] = [6, 0]$ is written as $2 \cdot 3 = 6$
$[2, 0] \oplus [0, 5] = [2, 5] = [0, 3]$ is written as $2 + (-5) = -3$
$[2, 0] \odot [0, 5] = [0, 10]$ is written as $2 \cdot (-5) = -10$
$[0, 2] \oplus [0, 3] = [0, 5]$ is written as $(-2) + (-3) = -5$
$[0, 2] \odot [0, 3] = [6, 0]$ is written as $(-2) \cdot (-3) = 6$

Incidentally, the above is one way to prove that there is a ring isomorphism betwen $\langle \mathbb{Z}, +, \cdot \rangle$ and $\langle \mathbb{I}, \oplus, \odot \rangle$, of course assuming that $\mathbb{Z}$ has already been constructed beforehand.

Subgraphs

Arthur Burlo'

Theorem 1 *Let H be a graph and K be a subgraph of H. Let $n(G)$ denote the number of vertices of a graph G and $k(G)$ denote the number of components of G. Then $n(K) - k(K) \leq n(H) - k(H)$.*

Proof:

We prove this by constructing H from K by adding edges and vertices.

Let $V_K = \{n_1, n_2, \ldots, n_p\}$ be the vertex set of K.
Let $E_K = \{e_1, e_2, \ldots, e_q\}$ be the edge set of K.

Also, let V_H and E_H be the vertex set and edge set of H.

Since K is a subgraph of H then $V_K \subseteq V_H$ and $E_K \subseteq E_H$. Let t be the number of vertices that are in V_H but not in V_K. In other words,

$$n(H) - n(K) = t$$

Add these t vertices to K to get graph K'. H and K' have the same vertices but H may have additional edges. If K has $k(K)$ components then K' has $k(K) + t$ components, since the additional t vertices that were introduced are not joined by edges to any of the other vertices already present in K (otherwise they would be vertices of K).

Since K' and H have the same set of vertices and all edges of K' (i.e. the edges of K) are in H then $k(H) \leq k(K')$. But

$$\begin{aligned} k(K') &= k(K) + t \\ &= k(K) + n(H) - n(K) \end{aligned}$$

Hence we obtain the result:

$$n(K) - k(K) \leq n(H) - k(H)$$

QED

Remark: $n(K) - k(K)$ is defined to be the . Thus we have proved that the removal of edges and/or vertices from a graph does not raise the .

Converse of Wilson's Theorem

Vincent Mercieca

Theorem 1 (Wilson's Theorem) *If p is prime, then $(p-1)! = -1$ mod p.*

Theorem 2 (Converse to Theorem 1) *If $(p-1)! = -1$ mod p, then p is prime.*

Lagrange's Proof of Theorem 2:

It is clear that every prime greater than 2 can be written in the form of $4m+1$ or $4m-1$.
If we assume that $4m+1$ is prime, $\Big((2m)!\Big)^2 = -1 \text{ mod } n \Rightarrow n$ is prime.
And, if $4m-1$ is prime, $(2m-1)! = \pm 1 \text{ mod } n \Rightarrow n$ is prime.

Let $n = 4m+1$, then

$$\begin{aligned} (n-1)! = (4m)! &= 1.2\cdots(2m)\cdots(4m) \\ \therefore (n-1)! \text{ mod } n &= 1.\dot{2}\cdots(2m)\cdots(4m) \text{ mod } (4m+1) \\ &= 1.2\cdots(2m)(-2m)\cdots(-1) \text{ mod } n \\ &= (-1)^{2m}.1.2\cdots(2m)(2m)\cdots 1 \text{ mod } n \\ &= \Big((2m)!\Big)^2 \text{ mod } n \end{aligned}$$

But $(n-1)! = -1 \text{ mod } n \Rightarrow \Big((2m)!\Big)^2 = -1 \text{ mod } n \Rightarrow n$ is prime.

Let $n = 4m-1$, then

$$\begin{aligned} (n-1)! = (4m-2)! &= 1.2\cdots(2m-1)(2m)\cdots(4m-2) \\ \therefore (n-1)! \text{ mod } n &= (2m-1)!(2m)\cdots(4m-2) \text{ mod } (4m-1) \\ &= (2m-1)!(-2m+1)\cdots(-1) \text{ mod } n \\ &= (-1)^{2m-1}\Big((2m-1)!\Big)^2 \text{ mod } n \\ &= -\Big((2m-1)!\Big)^2 \text{ mod } n \end{aligned}$$

$$\begin{aligned} \textit{But } (n-1)! = -1 \text{ mod } n &\Longrightarrow -\Big((2m-1)!\Big)^2 = -1 \text{ mod } n \\ &\Longrightarrow \Big((2m-1)!\Big)^2 = 1 \text{ mod } n \\ &\Longrightarrow (2m-1)! = \pm 1 \text{ mod } n \\ &\Longrightarrow n \text{ is prime.} \qquad \text{QED} \end{aligned}$$

Alternative proof:

Let $(n-1)! = -1 \bmod n$.
Then $\exists \lambda \in \mathbb{Z}$ *s.t.* $(n-1)! = \lambda n - 1 \Rightarrow \lambda n - (n-1)! = 1$

Suppose n is not prime.
Then $\exists a, b \in \{2, 3, \ldots, n-1\}$ *s.t.* $n = ab \Rightarrow n|(n-1)!$
Also $n|\lambda n$, hence $n|1$, which is a contradiction.

$\therefore n$ is prime. QED

Emails

Alexander Farrugia
Peter Borg

Subject: Write-up
Date: Sat, 4 Nov 2000 22:58:55 +0100
From: "Alexander Farrugia" <xact@nextgen.net.mt>
To: "Irene Sciriha" <isci1@um.edu.mt>

Hi Dr. Sciriha! This email is to notify you that my write-up will be sent to you next Monday 6th November. I'll also send a draft of my next item for the collection workshop. I don't know if it's interesting, but basically it's a construction of the integers Z from the natural numbers N. During the "Introductory Mathematics" course we learned the construction of Q from Z, R from Q and C from R, but we haven't done Z from N. I thought it would be interesting to fill that space :-D. It was actually inspired from an exercise from the book "Rings, Fields and Groups" by Allenby.

I'll email again next Monday to give my write-up and more details of my next item.

Regards,

Alex.

Subject: new proof!
Date: Fri, 10 Nov 2000 16:35:52 +0100
From: Peter Borg <pbor010@um.edu.mt>
Organization: University of Malta
To: irene@maths.um.edu.mt

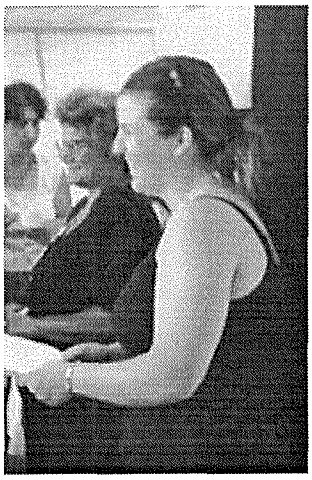
Dr. Sciriha,

I would like to tell you that I have another interesting proof which might be considered for a future workshop activity. It has to do with the divergence of the series 1 + 1/2 + 1/3 + 1/4 + ...
The proof is based on consideration of the series
1 + 1/3 + 1/3 + 1/3 + 1/9 + 1/9 + 1/9 + 1/9 + 1/9 + 1/9 + 1/9 +
1/9 + 1/9 + 1/27 + 1/27 + ... = 1 + 3(1/3) + 9(1/9) + 27(1/27)

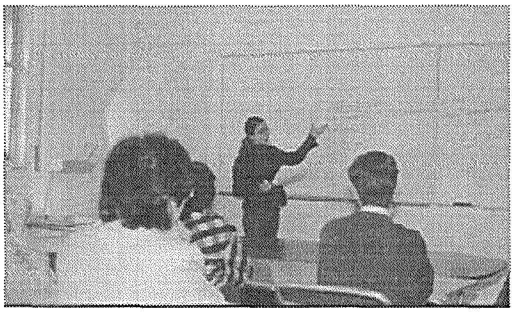
+ ... = 1 + 1 + 1 + ...
It can be shown that the latter series is less than the former, but since the latter diverges then the former diverges.

Peter.

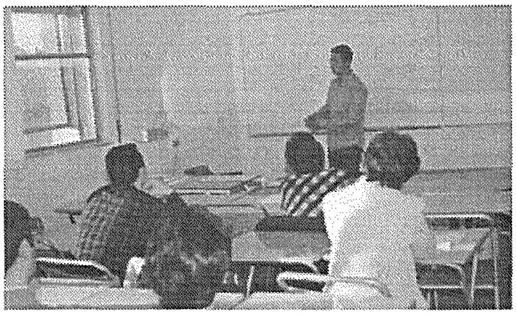
Dr. Irene Sciriha,
organiser of the workshop



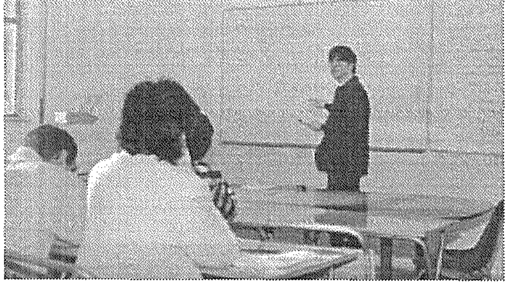
Ms. Annabelle Attard,
secretary



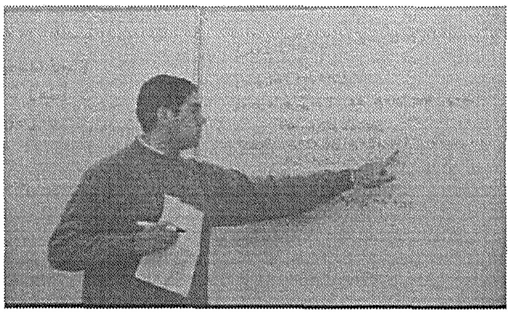
Ms. Louise Casha



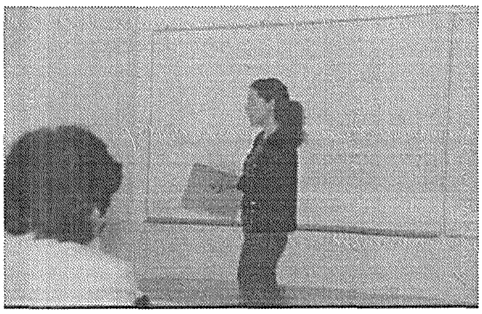
Mr. Peter Borg



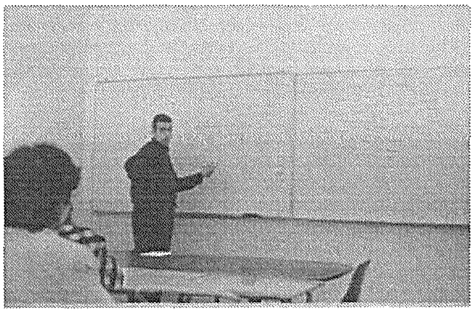
Mr. Arthur Burlo'



Mr. Alexander Farrugia



Ms. Fiona Farrugia



Mr. Vincent Mercieca

The audience