

PRELUDE MATHEMATICS

EDWARD O'CALLAGHAN

CONTENTS

1. Prelude	2
2. Introduction	2
3. Arithmetic	2
4. Numeral system	2
5. Construction of numbers	3
5.1. Divisibility	4
5.2. Higher dimensional numbers	5

1. PRELUDE

TODO: Fix notation here...

2. INTRODUCTION

In this course we build up the rudiments of high school mathematics.

3. ARITHMETIC

Arithmetic is derived from the Greek word, $\alpha\rho\iota\theta\mu\omicron\varsigma$, or “arithmos” or number. Arithmetic is the oldest known form of mathematical expression, dating back to 18,000BC, however still contains deep unsolved mysteries. The area of mathematics concerned with the study of such is known as *Number Theory*.

It should be clear from the history that there is actually no such thing as, say, “2” from a modern mathematical perspective. Many civilizations in antiquity had their own way of expressing numbers. For example, the ancient Egyptians had a little man with his hands waving in the air for one million. Not only did they express their numbers differently in script, they also counted in a different way. The differences in the way in which counting was done combined with is known as the script is now known as a **number system** which we shall come to shortly.

Now, no one has ever seen “2”, the script of “2” simply denotes a concept way off in ‘maths land’. For a more concrete example, take:

Example 3.1. $1 + 1 = 2$.

Notice that, we are actually say the *same thing* of both sides of the equality here. That is, $1 + 1$ points off in maths land to thing thing we call 2 and so does 2 and that by $=$ we mean they point at the same thing. Thus, given that mathematics is of course also a language, it does what you normally expect a language to do, repeat yourself until someone understands you. Hence, when you are off “solving” many problems here, consider that all you are actually doing is repeating yourself. By which you are taking out unnecessary things out of the argument at hand, distilling out the core argument (which we call the solution) in a clear way that others can follow. The hard part, as with all languages is that of construction, such that you are clear to others as to what you are thinking. Keep this prospective in mind when you are next stuck half way through an algebraic problem, where you are perhaps thinking, “what is the next right step”..

4. NUMERAL SYSTEM

A numeral system is really just a method of counting and denoting digits in a consistent manner. We are use to counting in the **base** ten number system with digits zero to nine. That is, take for example the number 3210 and see that:

Example 4.1. $3210 = (3) * 10^3 + (2) * 10^2 + (1) * 10^1 + (0) * 10^0$.

However, there is no particular reason we should count in base ten, we could count in base two with digits from zero to one, we call *bits*. This way of counting in base two is what we normally call binary. Taking say, 21 as an example, then:

Example 4.2. $(21)_{10} = ((1) * 2^4 + (0) * 2^3 + (1) * 2^2 + (0) * 2^1 + (1) * 2^0)_2$.

Keep this idea of *base* in mind when we do logarithms.

5. CONSTRUCTION OF NUMBERS

Now that we have established that a number is just a *representation* of an idea, this raises the question *what idea?* It turns out the best initial intuition of a number is from a geometric perspective. Consider the notation of 1 as a given unit line. Then, any positive number, say 3 is simply a multiple of this line, that is, you can view it as a **dilation**. Now, by multiplying any given line by -1 you can view this as making the line point or dilate in the opposite direction. This intuition may seem over the top at first however shall become useful when considering higher dimensional numbers in the form of a matrix, more on this later.

To construct the modern system in which we count, and in fact virtually all of mathematics, we must begin with the notion of a **set** as follows:

Definition 5.1. A set is a gathering together into a whole of definite, distinct objects of our perception and of our thought for which we called elements of the set.

If we take a set $X = \{1, 2, 3\}$ we can say $1 < 2$ and $2 < 3$ which implies $1 < 3$ if we impose a form of ordering denoted by $<$. The **natural** counting numbers, denoted by \mathbb{N} , is the classic one you are familiar with, where $\mathbb{N} = \{1, 2, 3, \dots\}$. Notice some algebraic properties of the naturals:

- Arithmetic addition is **closed**, that is, for any two elements $x, y \in \mathbb{N}$ then $x + y \in \mathbb{N}$;
- Arithmetic multiplication is closed, that is, for any two elements $x, y \in \mathbb{N}$ then $x * y \in \mathbb{N}$;
- Addition and multiplication are both commutative, e.g., for any two elements $x, y \in \mathbb{N}$ then $x + y = y + x$;
- Addition and multiplication are both associative, e.g., for any three elements $x, y, z \in \mathbb{N}$ then $x + (y + z) = (x + y) + z$;
- Multiplication is distributive over addition, that is, for any three elements $x, y, z \in \mathbb{N}$ then $x * (y + z) = x * y + x * z$;
- Identity of multiplication, that is, for any $x \in \mathbb{N}$ then $1 * x = x = 1 * x \in \mathbb{N}$.

Note. Do not always assume any of these are always true else where in mathematics in general! Such as, for example, commutativity.

You also should make note that the distributive law is like a kind of super glue that binds two different types of operations, addition and multiplication in this case, together. Also note that the order in which you do such acts on arguments you are making matters.

However we have a problem, we can not subtract since that it is not guarantied to be in the set, for example:

Example 5.2. $2 - 3 = -1 \notin \mathbb{N}$

Now, if we **adjoin** the notion of zero and negative, denoted by 0 and -1 respectively, to the naturals we form a new slightly larger set called the integers, denoted \mathbb{Z} . The word integer is Latin for “whole” and a \mathbb{Z} is used to denote them from the German word “zählen” which means “to count”. Hence, the integers is the set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ and that we now have the **existence** of identity of addition. That is, for any $x \in \mathbb{Z}$ then $x + 0 = x = 0 + x \in \mathbb{Z}$. We also have closure of subtraction, that is, for any $x, y \in \mathbb{Z}$ then $x + (-1 * y) = x - y \in \mathbb{Z}$.

OK, so we can now arithmetically add, subtract, multiply however division has yet to be **well-defined**. However, division seems like a **rational** thing we may like to do with numbers and so we form a new larger set from the integers called **the set of rationals** denoted by \mathbb{Q} . The \mathbb{Q} comes from the word **quotient**, from the Latin word “quotient” which is the result after division. Hence we **construct** the set of rationals \mathbb{Q} out of the set of integers \mathbb{Z} as follows:

Definition 5.3. $\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$

We should note that division by zero is **not** a **rational** thing to do and so this is part of our definition.

5.1. Divisibility. If a and b ($b \neq 0$) are integers, we say b *divides* a , or b is a divisor of a , if a/b is an integer. We shall denote by $b \mid a$ and conversely $b \nmid a$.

Example 5.4. $2 \mid 4$, however $3 \nmid 4$.

Example 5.5. If $a \in \mathbb{Z}$, then $1 \mid a$ and, for $a \neq 0$, then $a \mid a$; furthermore, $\forall a \in \mathbb{Z}^*, a \mid 0$.

Definition 5.6. A $p \in \mathbb{Z}^+ : p \neq 1$ is said to be **prime** iff p and 1 are the only divisors of p .

Example 5.7. 2, 3, 5, 7, 11, \dots

Definition 5.8. Given $x, y \in \mathbb{Z}^*$, then $d \in \mathbb{Z}$ is called the **greatest common divisor** of x and y if,

- $d > 0$,
- $d \mid x$ and $d \mid y$,
- $\forall f \in \mathbb{Z}^* : f \mid x \text{ and } f \mid y \text{ then } f \mid d$.

We denote the greatest common divisor d of both x and y by the $d = \gcd(x, y)$.

Example 5.9. $\gcd(341, 527) = 31$.

Definition 5.10. We say that x and y are **relatively prime** or **coprime** iff $\gcd(x, y) = 1$.

Note. Any two distinct primes are of course coprime.

Example 5.11. Given that $\gcd(27, 7) = 1$, then we see that 27 and 7 are coprime.

Lemma 5.12 (Euclid's Division Lemma).

$$\forall m(m > 0), p \in \mathbb{Z} \exists! q, r \in \mathbb{Z} : 0 \leq r < m \text{ and } p = qm + r$$

Note that we have simply rewritten a division problem in terms of multiplication and addition. Where, p is the dividend; m , the divisor; q , the quotient; and r , the remainder.

By Euclid's lemma we get the oldest known numerical algorithm still in use, Euclid's algorithm. Euclid's algorithm is simply the repeated application of Euclid's lemma.

Example 5.13. To find $\gcd(341, 527)$ we do the following;

$$\underline{527} = \underline{341} \cdot 1 + \underline{186}$$

$$\underline{341} = \underline{186} \cdot 1 + \underline{155}$$

$$\underline{186} = \underline{155} \cdot 1 + \underline{31}$$

$$\underline{155} = \underline{31} \cdot 5 + \underline{0}$$

Hence, $31 \mid 341$ and $31 \mid 527$ so $\gcd(341, 527) = 31$.

5.2. Higher dimensional numbers. Once again, recalling the profound yet simple notion of **representation**, we may represent the idea of higher dimensional numbers with the notation of **matrices**. For example, here is a two dimensional number one:

Example 5.14.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We call this special matrix, the **identity matrix** I . This can of course be generalised into n -dimensions.