

MATHEMATICS 1R  
DAVID PALAZZO (*Calculus*)  
GEORGIOS ANTONIOU (*Algebra*)

*Joao Almeida-Domingues\**

*University of Glasgow*

*September 17<sup>th</sup>, 2018 – November 30<sup>th</sup>, 2018*

CONTENTS

1	Properties of Numbers	2
1.1	Introduction . . . . .	2
2	Complex Numbers	7

---

\*2334590D@student.gla.ac.uk

## 1 PROPERTIES OF NUMBERS

## 1.1 Introduction

**1.1 definition.** A **set** is a finite or infinite collection of objects in which order has no significance, and multiplicity is generally also ignored

**1.2 notation.**  $A = \{a_1, a_2, a_3\}$

**1.3 notation.**  $a \in A$ , The element  $a$  belongs to the set  $A$

**1.4 notation.**  $A \subseteq B$ ,  $A$  is a subset of  $B$ , all elements of  $A$  appear in  $B$  but the opposite is not necessarily true

**1.5 notation.**  $A \subset B$ , the set  $B$  has at least one element which does not belong to  $A$

**1.6 notation.**  $a \notin A, A \not\subseteq B, A \not\subset B$ , are negations of the above

**1.7 definition.** **Natural Numbers**  $\mathbb{N}$ , the set of all positive whole numbers

**1.8 definition.** **Whole Numbers**  $\mathbb{N}_0$ ,  $\mathbb{N} + 0$

**1.9 definition.** **Integers**  $\mathbb{Z}$ ,  $\mathbb{N}_0 +$  negative whole numbers

**1.10 definition.** **Rational Numbers**  $\mathbb{Q}$ , the set of all fractions with denom  $\neq 0$

**1.11 definition.** **Irrational Numbers**  $\mathbb{R} \setminus \mathbb{Q}$ , the set of numbers which can not be expressed as a fraction

**1.12 definition.** **Real Numbers**  $\mathbb{R}$ , the set of all numbers in the real line

**1.13 remark.**  $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$  and  $\mathbb{R} \setminus \mathbb{Q} \subset \mathbb{R}$

**1.14 example.** Prove that  $\sqrt{n} \in \mathbb{R} \setminus \mathbb{Q}$ ,  $n > 1$  for any squarefree integer  $n$ , e.g.  $\sqrt{20}$

**Method**

1. Proof that any  $j \cdot g \in \mathbb{R} - \mathbb{Q}$ , with  $j, g \in \mathbb{Q}$ ,  $\mathbb{R} - \mathbb{Q}$
2. Decompose  $\sqrt{(n)}$  into  $k\sqrt{(u)}$ , where  $u$  is prime
3. Prove that  $\sqrt{(u)}$  is irrational by Euclid's Lemma Method

*Proof.*

Step 1 Let  $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$  and  $x \in \mathbb{R} - \mathbb{Q}$ :

$$(1) \quad x \cdot \frac{a}{b} = \frac{c}{d}$$

$$(2) \quad \iff x = \frac{cb}{da}$$

We reach a contradiction at (2) since integers are closed under addition, i.e.  $x$  must belong to  $\mathbb{Q}$

QED

*A set has closure under an operation if performance of that operation on members of the set always produces a member of the same set*

(Step 2)  $\sqrt{20} = 2\sqrt{5}$

*Proof.*

Step 3 It follows from ?? that  $2\sqrt{5}$  is rational iff 2 and  $\sqrt{5}$  are both rational.

Case 1: 2 is rational is trivially true

Case 2: Let's assume that  $\sqrt{5} \in \mathbb{Q}$ . This assumption implies that

$$\exists a, b \in \mathbb{Z}, b \neq 0 | \sqrt{5} = a/b$$

We can assume also that  $a/b$  is in its most reduced form, i.e. it has no common factors. Then,

$$(3) \quad \sqrt{5}^2 = \frac{a^2}{b^2}$$

$$(4) \quad 5b^2 = a^2$$

**1.15 lemma. Euclid's :** For a prime number  $p$  if  $p \mid mn$  then  $p \mid m$  or  $p \mid n$

It follows from 1.1 that 5 divides  $a^2$ . And from 1.15 (by setting  $p = 5, m, n = a$ ) that 5 divides  $a$ .

We then have that  $a = 5k, k \in \mathbb{Z}$ , and can therefore rewrite 1.1 :

$$(5) \quad 5b^2 = (5k)^2$$

$$(6) \quad b^2 = 5k^2$$

Similarly as above it follows then, that 5 divides  $b$ . Hence we reach the conclusion that 5 divides both  $a$  and  $b$ . Which contradicts our original assumption that  $a$  and  $b$  are coprime i.e. that  $\frac{a}{b}$  was in its most reduced form.

$\therefore \sqrt{5}$  is not irrational  $\implies \sqrt{20}$  is not irrational

QED

**1.16 lemma. Division Algorithm** Given two natural numbers  $a$  and  $b$ , there integers  $q$  and  $r$ , such that:

$$a = bq + r \quad q \geq 0 \text{ and } 0 \leq r < b$$

*Proof.* Let  $\frac{a}{b}$  be the positive natural number between  $q$  and  $q + 1$ .

$$q \leq \frac{a}{b} < q + 1$$

$$bq \leq a < bq + b$$

$$0 \leq a - bq < b$$

Setting  $r = a - bq$ , we obtain  $a = bq + r, q \geq 0$  and  $0 \leq r < b$  QED

**1.17 lemma. Euclidean Algorithm** is obtained by repeated application of 1.1.

$$\gcd(a, b) = am + bn$$

*Proof.*

$$1. \gcd(a, b) = \gcd(b, r) = \dots = \gcd(z, 0)$$

Why is this true?

If  $d|ab$ , then there exists a  $k, l$  s.t.  $a = dk$  and  $b = dl$  1.1 also tells us that  $a = bq + r$ , replacing  $dk$  and  $dl$ , we obtain the following:

$$dk = dlq + r$$

$$r = d(k - lq)$$

Hence, there exists a number (represented above by  $(k - lq)$ ) that multiplied by  $d$  gives us  $r$ . Therefore, by definition,  $d$  must also divide  $r$

2. Assuming that  $a > b > r$ , the sequence will decrease until eventually the remainder can not be further divided, i.e.  $r = 0$ . Hence,

$$\gcd(a, b) = \gcd(b, r) = \gcd(r, 0)$$

By looking at the last term of the equality we find that the gcd must by definition be  $r$  (since it divides exactly). Therefore, by back-substituting the result <sup>1</sup> we find that the **gcd of the original expression is equal to the remainder of the penultimate**

QED

---

<sup>1</sup>recursively, haskell style

**1.18 example.** Find integers  $m$  and  $n$  such that  $55m + 7n = 1$ . Note that by the definition of the division algorithm, if such numbers exist, then we expect  $\gcd(55, 7) = 1$ . So, we start by applying the division algorithm to verify that it exists:

$$55 = 7 \cdot 7 + 6$$

$$7 = 6 \cdot 1 + 1$$

$$6 = 1 \cdot 6 + 0$$

We can now rearrange the equations above in the form  $r = a - bq$ , and backtrack until we reach the original equation in terms of 55 and 7.

$$6 = 55 - 7 \cdot 7$$

$$1 = 7 - 6 \cdot 1$$

$$= 7 - (55 - 7 \cdot 7)(1)$$

$$= 7(8) - 55$$

Hence,  $m = -1$  and  $n = 8$

**1.19 definition.** **Polynomial** of degree  $n \geq 0$  is an expression of the form:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

Where  $a_n$  is the leading coefficient

**1.20 remark.** If  $a_n = 1$ , then the polynomial is said to be monic

**1.21 remark.** 0 is considered to be a polynomial

**1.22 remark.** The Euclidean Algorithm can also be applied to polynomials, since:

$$f(x) = g(x)q(x) + r(x)$$

Where  $0 \leq r(x) < g(x)$

**1.23 theorem. Remainder:** Let  $f(x)$  be a polynomial in  $x$ , and  $c$  be a constant:

$$f(x) = (x - c)q(x) + f(c)$$

**1.24 theorem. Factor:** If  $f(c) = 0$ , then  $(x - c)$  is a factor of  $f(x)$

**1.25 example.** Find the highest monic quadratic polynomial which divides both

$$g(x) = x^3 + 6x^2 + 11x + 6 \text{ and } f(x) = x^4 + 5x^3 + 10x^2 + 20x + 24$$

Following a similar procedure as before, we can apply the Euclidean Algorithm until we find a polynomial which divides  $g(x)$  and  $f(x)$  exactly (i.e.  $r(x) = 0$ ). The key point is to keep in mind the fact that **any polynomial which divides both  $f(x)$  and  $g(x)$  must also divide their remainder.**

1. Dividing  $f(x)$  by  $g(x)$ , so as to find  $q(x)$  and  $r(x)$ :

$$\begin{array}{r} x - 1 \\ x^3 + 6x^2 + 11x + 6 \overline{) x^4 + 5x^3 + 10x^2 + 20x + 24} \\ \underline{-x^4 - 6x^3 - 11x^2 - 6x} \phantom{+ 24} \\ -x^3 - x^2 + 14x + 24 \\ \underline{x^3 + 6x^2 + 11x + 6} \\ 5x^2 + 25x + 30 \end{array}$$

Hence, we have that:

$$f(x) = g(x)(x - 1) + 5(x^2 + 5x + 6)$$

2. Continuing the algorithm, now with  $g(x)$  and monic  $r(x)$  obtained above:

$$\begin{array}{r} x + 1 \\ x^2 + 5x + 6 \overline{) x^3 + 6x^2 + 11x + 6} \\ \underline{-x^3 - 5x^2 - 6x} \phantom{+ 6} \\ x^2 + 5x + 6 \\ \underline{-x^2 - 5x - 6} \\ 0 \end{array}$$

Since the remainder is 0, we find that  $(x^2 + 5x + 6)$  divides exactly into  $g(x)$ , and therefore also divides into  $f(x)$ . Lastly, by looking at the remainder of the penultimate iteration, we can assert that,  $x^2 + 5x + 6$  is the highest monic polynomial which divides both  $f(x)$  and  $g(x)$

## 2 COMPLEX NUMBERS