m3pm16l2.tex
Lecture 1. 17.1.2012

Chapter I. PRELIMINARIES

1. PRIMES. Recall (M2PM3, I.2) $\mathbb{N} := \{1, 2, 3, ...\}$, the set of *natural numbers*. Also, $\mathbb{N}_0 := \{0, 1, 2, ...\} = \mathbb{N} \cup \{0\}$. We can take these for granted, or proceed as follows (John von NEUMANN (1903-57) in 1923):

$$0 \longleftrightarrow \emptyset; \quad 1 \longleftrightarrow \{\emptyset\}; \quad 2 \longleftrightarrow \{0, 1\}; \quad 3 \longleftrightarrow \{0, 1, 2\}; \quad \text{etc.}$$

Addition comes with $\mathbb{N}$. Its inverse, subtraction, gives

$$\mathbb{Z} := \{..., -3, -2, -1, 0, 1, 2, 3, ...\} \qquad \text{(integers – Z for Zahl)},$$

an additive group. We can multiply integers, and divide *non-zero* integers, leading to the *rationals*:

$$\mathbb{Q} := \{m/n : m, n \in \mathbf{Z}, n \neq 0\} \qquad \text{(Q for quotient)}.$$

The ancient Greeks had $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$. We meet the reals $\mathbb{R}$ as:
(i) lengths of line segments (as in Greek geometry);
(ii) infinite decimal expansions.
Constructing $\mathbb{R}$ from $\mathbb{Q}$ is hard, and was not done till 1872, in two ways:
(i) *Dedekind cuts* (or *sections*): Richard DEDEKIND (1831-1916);
(ii) *Cauchy sequences*: Georg CANTOR (1845-1918).
Dedekind cuts are specific to $\mathbf{R}$, as they depend on the *total ordering* of the line ("$x < y, x > y$ or $x = y$"). Cauchy sequences are general, and can be done in any *metric space*.
Then getting $\mathbb{C}$ from $\mathbb{R}$ is easy (Argand diagram: M2PM3, I.1).

The subject of Number Theory (NT) splits several ways:
Analytic v. algebraic. We develop Analytic Number Theory (ANT) using Analysis, specifically Complex Analysis (M2PM3, NHB); Algebraic Number Theory concerns rings, ideals, field extensions (Galois theory), etc.

There is also *Elementary Number Theory* (ENT). Here 'elementary' does *not* mean 'easy', but 'without using preliminaries such as Complex Analysis – which (if one knows Complex Analysis, as we do) is harder.
Multiplicative v. Additive. This course is on Multiplicative Number Theory – concerning multiplicative aspects such as primes. Additive Number Theory

concerns, e.g., Goldbach's Conjecture (is every even integer $n > 2$ the sum of two primes?), Waring's Problem, etc.

Theorem (FUNDAMENTAL THEOREM OF ARITHMETIC, FTA). Every integer $n \geq 2$ can be written uniquely (to within order) as a product of prime factors.

Proof. Existence. Induction. True for $n = 2$. Assume true for every integer $< n$. If n is not prime (i.e. is composite), it has a non-trivial divisor d $(1 < d < n)$. So $n = cd$ $(1 < c < n)$. So each of c, d is a product of primes, by the inductive hypothesis. So n is too, completing the induction.
Uniqueness. Induction. True for $n = 2$. Assume true for every integer $< n$. If n is prime, the result holds, so assume n is composite. If it has two factorisations

$$n = p_1 \dots p_r = q_1 \dots q_s,$$

to show $r = s$ and each p is some q. As p_1 is prime and divides the product $n = q_1 \dots q_s$, it must divide at least one factor (w.l.o.g., q_1): $p_1 | q_1$. Then $p_1 = q_1$ as both p_1, q_1 are prime. Cancel p_1:

$$n/p_1 = p_2 \dots p_r = q_2 \dots q_s.$$

As n is composite, $1 < n/p_1 < n$. Then the inductive hypothesis tells us that the two factorisations above of n/p_1 agree to within order: $r = s$, and $p_2, \dots, p_r$ are $q_2, \dots, q_r$ in some order, as required. //

Historical Note. We owe Mathematics as a subject to the ancient Greeks. Of the 13 books of Euclid's Elements (EUCLID of Alexandria, c. 300 BC), three (Books VI, IX and X) are on Number Theory. From the ordering of the material in Euclid, it is clear that the Greeks knew that they did not have a proper theory of irrationals (i.e. reals). Although they did not state FTA, it had been assumed that they "knew it really", but did not state it explicitly. This view is contradicted by Salomon BOCHNER (1899-1982) (*Collected Papers*, Vol. 4, AMS, 1992). According to Bochner, the Greeks did *not* know FTA, nor have a notational system adequate even to state it!

L. E. DICKSON (1874-1954) (*History of the Theory of Numbers* Vols 1-3, 1919-23) does not address the question of the Greeks and FTA!

The first clear statement and proof of FTA is in Gauss' thesis (C. F. GAUSS (1777-1855); *Disquisitiones Arithmeticae*, 1798, publ. 1801).