Math 300 Class 1

Monday 7th January 2019

Definition 1 — *Propositions and proofs*
A **proposition** is a statement to which it is possible to assign a **truth value** ('true' or 'false'). If a proposition is true, a **proof** of the proposition is a logically valid argument demonstrating that it is true, which is pitched at such a level that a member of the intended audience can verify its correctness.

Exercise 2
Think of an examples of (a) a true proposition, (b) a false proposition, (c) a proposition whose truth value you don't know, and (d) a statement that is not a proposition.

(a) 2 is an even number

(b) 2 is an odd number

(c) Every even integer greater than two is the sum of two positive primes.

(d) This sentence is false.

One of the most fundamental concepts in all of pure mathematics is that of a *set*.

Definition 3 — *Sets and elements (informal definition)*
A **set** is a collection of objects. The objects in the set are called **elements** of the set. If X is a set and x is an object, then we write $x \in X$ to denote the assertion that x is an element of X.

We will study sets abstractly soon. For now, we consider the following concrete examples:

- The set $\mathbb{N}$ of **natural numbers**: $0, 1, 2, 3, \ldots$
- The set $\mathbb{Z}$ of **integers**: $\ldots, -2, -1, 0, 1, 2, \ldots$
- The set $\mathbb{Q}$ of **rational numbers**, which are numbers of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$;
- The set $\mathbb{R}$ of **real numbers**, which are arbitrary points on the 'number line'.

So for example, '$5 \in \mathbb{Z}$' means '5 is an integer', and '$\frac{1}{2} \in \mathbb{Q}$' means '$\frac{1}{2}$ is a rational number'.

Definition 4 — *Division of integers*
An integer b **divides** an integer a if there is an integer q such that $qb = a$.

For example, 4 divides 12, since $3 \times 4 = 12$.

Exercise 5
Given any integer a, prove that 1 divides a and that a divides 0.

$a = a \times 1$, so 1 divides a by Def 4

$0 = 0 \times a$, so a divides 0 by Def 4

Proposition 6
Let a, b and c be integers. If c divides b and b divides a, then c divides a.

Proof

c divides b $\Rightarrow$ $b = qc$ for some $q \in \mathbb{Z}$

b divides a $\Rightarrow$ $a = rb$ for some $r \in \mathbb{Z}$

Substituting qc for b gives $a = r(qc) = (rq)c$

Since $rq \in \mathbb{Z}$, c divides a by Def 4.

$\square$

Theorem 7 — *Division theorem*
Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There is exactly one way to write

$$a = qb + r$$

such that q and r are integers, and $0 \leqslant r < |b|$.

The integer q is called the **quotient** and the integer r is called the **remainder**.

Proposition 8
Let $a, b \in \mathbb{Z}$ with $b > 0$, and suppose that a leaves a remainder $r > 0$ when divided by b. Then $-a$ leaves a remainder of $b - r$ when divided by b.

Proof

Since a leaves a remainder of r when divided by b, we have $a = qb + r$ for some $q \in \mathbb{Z}$.

Moreover $0 < r < b$ since r is a remainder and $r > 0$.

Now
$$\begin{aligned} -a &= -(qb+r) \\ &= -qb - r \\ &= -(q+1)b + (b-r) \end{aligned}$$

and $\begin{cases} b - r > 0 & \text{since } r < b \\ b - r < b & \text{since } r > 0 \end{cases}$

so $b - r$ is the remainder of $-a$ when divided by b.

□

Pre-class assignment for Class 2 (Tue, Jan 8)

Read the course syllabus carefully and then fill out the following questionnaire:

`https://goo.gl/forms/U4qtK3yhDXNWiP3m2`

The syllabus and questionnaire can both be found on Canvas (go to Assignments → Class 2).