FROM LECTURE 1: WELLORDERING PRINCIPLE AND DIVISION WITH REMAINDER

Why is this document in English? Because it is reasonable to assume that within a few years, Bachelor level courses at the University of Copenhagen will be taught in English (again). To avoid having to translate additional course material when this (inevitably) happens, I am going to write most of my supplementary notes in English. As a further upside, you will get used to reading math in English, which will be an advantage later on in your studies.

The Wellordering principle. Recall from lecture that

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

and that[1]

$$\mathbb{N}_0 = \omega = \{0, 1, 2, 3, 4, \ldots\}.$$

All the ordinary rules of addition and multiplication hold in $\mathbb{N}$ and $\mathbb{N}_0$, but when forming the additive inverse (i.e., $-x$) and the multiplicative inverse (i.e., x^{-1}), we may be falling outside of these sets and into $\mathbb{Z}$ (the integers) or $\mathbb{Q}$ (the rationals). (E.g. $5 \in \mathbb{N}$, but $-5 \notin \mathbb{N}$, and $5^{-1} \in \mathbb{Q}$ but $5^{-1} \notin \mathbb{N}$.) This is not a usually a huge concern, but if one is trying to solve an equation within $\mathbb{N}$, say, then this can become a concern.

A key feature of the ordering of the natural numbers is the *wellordering principle*, also called the *wellordering axiom*. (Dansk: *Velordningsprincippet* eller *velordningsaksiomet*.) It says the following:

Wellordering principle: If $X \subseteq \mathbb{N}_0$ is a a non-empty (!) set, then X contains a least element. That is, if $X \subseteq \mathbb{N}_0$ is non-empty then there is $x \in X$ such that for all $y \in X$ we have $x \leq y$.

The same holds for $\mathbb{N}$ instead of $\mathbb{N}_0$, of course. The wellordering principle is a fundamental assumption about the natural numbers, i.e., it is an axiom in the true sense of the word. It cannot be proven by appealing to algebraic properties of $\mathbb{N}$, for instance. It must be assumed from the beginning.

The division with remainder theorem. In lecture, we used the wellordering principle to give a proof of the following important theorem, called the *division with remainder theorem.*

Theorem 1. *Let $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are $q_0 \in \mathbb{Z}$ and $r_0 \in \mathbb{N}_0$, with $0 \leq r_0 < d$, such*

$$a = dq_0 + r_0.$$

Moreover, the q_0 and r_0 satisfying the above are unique.

[1] The notation ω for $\mathbb{N}_0$ is preferred by mathematical logicians. Mathematicians outside of logic are usually not accustomed to this use of ω. Also, many mathematicians use $\mathbb{N}$ for what we call $\mathbb{N}_0$, so beware!

The wellordering principle is crucial for the proof of this theorem, though its use is somewhat swept under the rug in the DIS textbook. Nonetheless, you should still read the proof there, since it may seem a bit more intuitive than what I do here.

Proof of Theorem 1. For simplicity, we shall first give the proof assuming that $a > d > 0$. We start by proving a simple claim (dansk: påstand), which gets the wellordering principle into play.

Claim. The set $M = \{q \in \mathbb{N} : a - dq \leq 0\}$ is non-empty.

Proof of claim. Since $d \geq 1$ by our assumption, it follows that $ad \geq a$. So if we let $q = a$ then $a - dq \leq 0$. (Claim)⊣

Now let $q_0 \in M$ be the least element of M. It suffices to prove that $r_0 = dq_0 - a$ works, i.e., that $0 \leq r_0 < d$. For this, first note that $q_0 > 1$, since if $q_0 = 1$ was the case then $a - d \leq 0$, whence $a \leq d$, contradicting our assumption that $a > d$. So suppose then that $r_0 \geq d$. Then $r_0 - d \geq 0$, and so $(dq_0 - a) - d \geq 0$. This then amounts to

$$0 \geq (dq_0 - a) - d = d(q_0 - 1) - a$$

from which we get $a - d(q_0 - 1) \leq 0$. But since $q_0 > 1$ we have $q_0 - 1 \in \mathbb{N}$, which then contradicts that q_0 was the least natural number such that $a - dq_0 \leq 0$.

This finishes the proof of the existence part of the theorem, as we have produced q_0 and r_0 as required.

For the uniqueness part, suppose that $q' \in \mathbb{Z}$ and $r' \in \mathbb{N}_0$, with $0 \leq r' < d$, also satisfy $a = dq' + r'$. A simple calculation shows that if $q = q'$ then $r = r'$, so we may assume, seeking a contradiction, that $q' \neq q$. Note that $dq' - r' \leq 0$ and so $q' \in M$, whence by minimality of q_0 we have $q' > q_0$, in particular, $q' \geq q_0 + 1$. It then follows that $dq' \geq dq_0 + d > a$, with the last inequality following since $r < d$ gives $a = dq_0 + r < dq_0 + d$. But then $dq' - a > 0$, which contradicts that $q' \in M$.

This finishes the proof of the theorem in the case $a > d > 0$. We leave it as an exercise (see below) to prove the theorem without this assumption. □

Exercise 1. Use the fact that the division with remainder theorem holds for $a > d > 0$ to prove that it holds for all $a \in \mathbb{Z}$ and $d \in \mathbb{N}$.

Exercise 2. On the face of things, the above proof seems very different from the proof of the same theorem given in the textbook, in particular the existence part. However, a closer look should reveal that the idea is exactly the same. Explain, in your own words and using everyday language, what is going on in (the existence part of) the two proofs, and why the idea is actually the same. (Hint: I suggest that you start by explaining the idea behind Jesper Lützen's proof, and then use this to explain the idea behind the above proof.)