3. Mathematical induction. Axioms of integers. Division Algorithm.

3.1. **Mathematical induction.** The general setup where the method of mathematical induction may be applicable is as follows. Suppose that for every $n \in \mathbb{N}$ we are given some statement $P(n)$, depending on n, e.g.

$$1 + \ldots + n = \frac{n(n+1)}{2} \qquad P(n).$$

The statement may have the form of an equality, inequality or something more involved. We wish to prove that $P(n)$ is true for all $n \in \mathbb{N}$. The method of mathematical induction asserts that this can be accomplished in two stages:

(i) (Induction base) Prove that $P(1)$ is true

(ii) (Induction step) For every $n \in \mathbb{N}$ prove the implication "$P(n) \Rightarrow P(n+1)$", that is, assume that $P(n)$ is true and deduce that $P(n+1)$ is true.

Indeed, if we verified (i) and (ii), then the following sequence of implications shows that $P(n)$ must be true for all $n \in \mathbb{N}$:

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \ldots$$

Example 3.1. *Prove that* $1 + \ldots + n = \frac{n(n+1)}{2}$ *for all* $n \in \mathbb{N}$.

For simplicity of notation in this example we let $s_n = 1 + \ldots + n$. Thus the statement $P(n)$ we have to prove in this problem can be rewritten as

$$s_n = \frac{n(n+1)}{2} \qquad P(n)$$

Note that by definition $s_1 = 1$ and $s_{n+1} = (1 + \ldots + n) + (n+1) = s_n + (n+1)$. The conditions $s_1 = 1$ and $s_{n+1} = s_n + (n+1)$ for all $n \in \mathbb{N}$ completely determine the sequence $\{s_n\}$, so from this point on we can forget about the original definition of s_n and work with this recursive definition.

Base case: $n = 1$. We need to check that $s_1 = \frac{1(1+1)}{2}$. This is true since $s_1 = 1$ by definition and $\frac{1(1+1)}{2} = 1$ as well.

Induction step. "$P(n) \Rightarrow P(n+1)$". Now we fix n and assume that $s_n = \frac{n(n+1)}{2}$. Our goal is to show that $s_{n+1} = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$.

We shall compute both s_{n+1} and $\frac{(n+1)(n+2)}{2}$ and show that they are equal to each other. Multiplying out, we have $\frac{(n+1)(n+2)}{2} = \frac{n^2+3n+2}{2} = \frac{n^2}{2} + \frac{3n}{2} + 1$. On the other hand, using the recursive relation $s_{n+1} = s_n + (n+1)$ and the

inductive hypothesis $s_n = \frac{n(n+1)}{2}$, we get

$$s_{n+1} = s_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2}{2} + \frac{n}{2} + n + 1 = \frac{n^2}{2} + \frac{3n}{2} + 1.$$

Thus, we proved that $s_{n+1} = \frac{(n+1)(n+2)}{2}$, so $P(n+1)$ is true. This completes the induction step.

Example 3.2. *Prove that for every* $n \in \mathbb{N}$

$$\textit{there exist } a_n, b_n \in \mathbb{Z} \textit{ such that } (1+\sqrt{2})^n = a_n + b_n\sqrt{2}. \qquad P(n)$$

In this problem the statement $P(n)$ is more complicated as it does not specify the values of a_n and b_n (they are for us to choose; all we have to make sure is that $a_n, b_n \in \mathbb{Z}$). We shall solve this problem by induction as follows: first we will define $a_1, b_1 \in \mathbb{Z}$ so that $P(1)$ is true. Then, for every $n \in \mathbb{N}$, we will assume that $P(n)$ is true and then define a_{n+1} and b_{n+1} recursively in terms of a_n and b_n so that $P(n+1)$ is true.

Base case: $n = 1$. We set $a_1 = b_1 = 1$. Then $a_1 + b_1\sqrt{2} = 1 + \sqrt{2} = (1+\sqrt{2})^1$, so $P(1)$ is true.

Induction step. Now assume that $P(n)$ is true, so that $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$ for some $a_n, b_n \in \mathbb{Z}$. Before defining a_{n+1} and b_{n+1}, we compute $(1+\sqrt{2})^{n+1}$ using the above formula for $(1+\sqrt{2})^n$. We have

$$(1+\sqrt{2})^{n+1} = (1+\sqrt{2})^n \cdot (1+\sqrt{2}) = (a_n + b_n\sqrt{2})(1+\sqrt{2}) = (a_n+2b_n) + (a_n+b_n)\sqrt{2}.$$

Now it is clear how to define a_{n+1} and b_{n+1}: we set $a_{n+1} = a_n + 2b_n$ and $b_{n+1} = a_n + b_n$. Then $(1+\sqrt{2})^{n+1} = a_{n+1} + b_{n+1}\sqrt{2}$ by the above computation. Also, since $a_n, b_n \in \mathbb{Z}$ by inductive hypothesis and since integers are closed under addition and multiplication by 2, we conclude that $a_{n+1}, b_{n+1} \in \mathbb{Z}$. Thus, we verified that $P(n+1)$ is true.

Here are a few standard variations one sometimes needs to make when doing an induction proof.

(i) Sometimes it is technically more convenient to do the induction step in the form "$P(n-1) \Rightarrow P(n)$" (instead of $P(n) \Rightarrow P(n+1)$). Of course, in this case we assume that $n \geq 2$ in the induction step.

(ii) We may be asked to prove that certain statement $P(n)$ holds for all integers $n \geq a$ for some $a \neq 1$. In this case proof by induction works the same except that in the base case we verify $P(a)$, not $P(1)$.

(iii) It is possible that the statement $P(n)$ holds for all $n \in \mathbb{N}$, but the natural argument for the induction step does not work for some small values of n (say, it only works for $n \geq 3$). In this case we verify $P(1), P(2)$ and $P(3)$ separately as part of the base case.

(iv) Finally, sometimes we need to use the *complete induction* (or *strong induction* in Pinter's terminology). In this case, for the induction step we assume not only that $P(n)$ is true but that $P(k)$ is true for all $k \leq n$ (that is, $P(1), P(2), \ldots, P(n)$ are all true) and deduce that $P(n+1)$ is true. Note that the logical justification of a proof by complete induction remains the same.

3.2. **Axioms of integers.** Over the next few lectures we will study arithmetic properties of integers (as usual denoted by $\mathbb{Z}$) – here by arithmetic properties we mean properties dealing with concepts like divisibility, greatest common divisor, prime factorization, congruences etc.

We will begin by stating axioms of integers. We will not aim to deduce every single property of integers we shall need from these axioms and will allow ourselves to use some very basic properties of integers (which you would normally consider completely obvious) without explicitly showing how they follow from axioms (typical examples of such properties are mentioned below). However, we shall try to give complete proofs for all arithmetic properties of integers (in the sense of the previous paragraph).

There are three groups of axioms of integers, denoted below by (Z1)-(Z3). The first two groups of axioms have already been discussed (in a broader context) in Lectures 1 and 2.

(Z1) $\mathbb{Z}$ is a commutative ring with 1

(Z2) $\mathbb{Z}$ is an ordered ring.

Note that while both (Z1) and (Z2) are formally stated as a single property, unwinding the definitions of a commutative ring with 1 and ordered ring, respectively, we see that both (Z1) and (Z2) combine several properties.

The third group (Z3) contains just one axiom, usually known as a well-ordering principle:

(Z3) (Well-ordering principle) Let $\mathbb{Z}_{>0} = \mathbb{N}$ denote the set of all positive integers. Then every non-empty subset of $\mathbb{Z}_{>0}$ has the smallest element. In other words, if $S \subseteq \mathbb{Z}_{>0}$ is any non-empty subset, then there exists $m \in S$ such that $m \leq x$ for all $x \in S$.

Remark: 1. The statement of the well-ordering principle remains true if $\mathbb{Z}_{>0} = \mathbb{N}$ is replaced by $\mathbb{Z}_{\geq 0}$, the set of all non-negative integers (this claim is left as an exercise). Sometimes it will be more convenient to use this version of the well-ordering principle.

2. Note that the well-ordering principle would become false if we replace $\mathbb{Z}_{>0}$ by $\mathbb{Q}_{>0}$ (positive rationals) or $\mathbb{R}_{>0}$ (positive reals). Indeed, the set

of all positive rationals has no smallest element since for every $q \in \mathbb{Q}_{>0}$ the number $\frac{q}{2}$ is an element of $\mathbb{Q}_{>0}$ which is less than q. The well-ordering principle would also become false if we replace positive integers by all integers (the set of all integers has no smallest element). Finally, we do not need to assume that the subset S in (Z3) is non-empty, as the empty set has no elements at all, and in particular it has no smallest element.

We now proceed by stating a few additional (intuitively obvious) properties of integers which we will accept without proof (even though it does not make much work to deduce them from (Z1)-(Z3)).

Induction Property: Let S be a subset of $\mathbb{N}$ satisfying the following two conditions:

(i) $1 \in S$

(ii) $n \in S \Rightarrow n + 1 \in S$ for every $n \in \mathbb{Z}_{>0}$

Then $S = \mathbb{N}$.

If we go back to our description of the principle of mathematical induction and look at the justification provided, we will see that what we implicitly used is precisely the induction property above.

It is not hard to show that the induction property is equivalent to the well-ordering principle, that is, the well-ordering principle implies the induction property and vice versa the induction property implies the well-ordering principle. For this reason it is common to replace the well-ordering principle by the induction property in the list of axioms of integers.

Here are some additional properties that we shall commonly use without explicit reference:

(i) $n \geq 1$ for every $n \in \mathbb{N}$.

(ii) For every $n \in \mathbb{N}$ there are only finitely many $m \in \mathbb{N}$ such that $m \leq n$.

Property (i) is very easy to prove by induction, and it takes a bit more work to formally prove (ii).

3.3. **Division with remainder (aka division algorithm).** We finish this lecture by proving the theorem about division with remainder for integers.

Theorem 3.3 (Division with remainder)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r \leq |b| - 1$. As usual, q is called the quotient and r is called the remainder.*

Proof. As with any theorem whose statement starts with "There exists unique ...", the proof consists of two parts – the existence part and the uniqueness part. It is not difficult to prove Theorem 3.3 using only axioms (Z1)-(Z3); however we will give a slightly different proof. Our proof will not

be entirely self-contained as we will assume some basic properties of real numbers, but has the advantage of being slightly more intuitive.

Existence: It is convenient to divide the proof into two cases: $b > 0$ and $b < 0$.

Case 1: $b > 0$. Given a real number x, denote by $[x]$ the *integer part of* x. By definition $[x]$ is the largest integer which is $\leq x$. It is clear from this definition that

$$[x] \leq x < [x] + 1 \qquad (***)$$

Define $q = [\frac{a}{b}]$ and $r = a - bq$. Then it is clear that q and r are integers and $a = bq + r$. The only thing we need to check is that r satisfies the double inequality $0 \leq r \leq b - 1$.

Since $q = [\frac{a}{b}]$ by definition, applying (***) with $x = \frac{a}{b}$ we get $q \leq \frac{a}{b} < q+1$. Since $b > 0$, we can multiply by b to get $bq \leq a < b(q + 1) = bq + b$. Subtracting bq, we get $0 \leq a - bq = r < b$. Finally, since r and b are both integers, $r < b$ implies that $r \leq b - 1$.

Thus, we proved that $0 \leq r \leq b - 1$, as desired.

Case 2: $b < 0$. We will give a proof USING the result of Case 1.

Since $b < 0$, we have $-b > 0$, so we can apply the result of case 1 with a and b replaced by $-a$ and $-b$, respectively. We get that there exist $q', r' \in \mathbb{Z}$ such that $-a = (-b)q' + r'$ with $0 \leq r' < |-b| = |b|$.

Multiplying both sides by -1, we get $a = bq' + (-r')$. Note that this is not the final answer since r' is not in right range. Indeed, since $0 \leq r' < |b|$, we have $-|b| < -r' \leq 0$. But this problem is easy to fix.

If $r' = 0$, then $a = bq'$, so we are done setting $q' = q$ and $r = 0$. If $r' \neq 0$, we set $q = q' + 1$ and $r = -r' - b$. Then $bq + r = b(q' + 1) + (-r' - b) = bq' + (-r') = a$. We know that $-|b| < -r' \leq 0$; this can be rewritten simply as $b < -r' \leq 0$ (since $b < 0$, we have $|b| = -b$). We also assume that $r' \neq 0$, so $b < -r' < 0$. Subtracting b, we get $0 < -r' - b < -b$ or, equivalently, $0 < r < |b|$, which finishes the proof of the existence part.

Uniqueness: To prove uniqueness, we assume that there exist two distinct pairs (q, r) and (q', r') satisfying the desired conditions and reach a contradiction.

So assume that there exist $q, q', r, r' \in \mathbb{Z}$ such that $a = bq + r = bq' + r'$, $0 \leq r, r' < |b|$ and $(q, r) \neq (q', r')$.

The equality $bq+r = bq'+r'$ can be rewritten as $b(q-q') = r'-r$. Taking absolute values of both sides and using the formula $|xy| = |x| \cdot |y|$, we get $|b| \cdot |q - q'| = |r' - r|$.

Since r' and r both lie in the half-open interval $[0, |b|)$, the distance between r' and r must be less than $|b|$ (the length of the interval), so $|r' - r| < |b|$. We proceed by splitting the argument into two cases.

Case 1: $q \neq q'$. Then $|q - q'| > 0$, so $|q - q'| \geq 1$ and therefore, $|r' - r| = |b| \cdot |q - q'| \geq |b| \cdot 1 = |b|$. This contradicts the earlier inequality $|r' - r| < |b|$.

Case 2: $q = q'$. Then from $b(q - q') = r' - r$ we get that $r' = r$. So the pairs (q, r) and (q', r') are the same, which contradicts the initial hypothesis that they are distinct.

□

3.4. **Book references.** The references for this lecture are as follows:

3.1 is covered in [Gilbert, 2.2] and [Pinter, Ch.21]

3.2 is covered in [Gilbert, 2.1] and [Pinter, Ch.21], but in both cases the approach is slightly different

3.3 is covered in [Gilbert, 2.3] and [Pinter, Ch.21]. Both books give a different proof of the division algorithm which does not use real numbers.