CMSC 27130: Honors Discrete Mathematics

Lectures by Alexander Razborov
Notes by Geelon So, Isaac Friend, Warren Mo

University of Chicago, Fall 2016

Introduction

The following notes were hand-written and considerably edited. Much of the instructor's original exposition remains preserved, however. The scribe for each lecture is responsible for all errors in this document.
Errata should be addressed to warrenmo@uchicago.edu.

Acknowledgements

A huge debt of gratitude is owed to Nitin Krishna for providing me with the LaTeX code in which these notes arer typesetted.

References

The primary reference is [4].

[1] L. Lovasz. *Combinatorial Problems and Exercises*, AMS Chelsea Publishing, 2007.

[2] J. Matousek, J. Nesetril. *An Invitation to Discrete Mathematics*, Oxford University Press, 2009.

[3] E. Mendelson. *Introduction to Mathematical Logic*, CRC Press, 2015.

[4] K. Rosen. *Discrete Mathematics and its Applications*, McGraw-Hill Education, 2007.

Lecture 1 (Monday, September 26)

▶ Mathematical Induction

We let $P(n)$ for $n \geq 1$ to be some statement. Using **mathematical induction**, our goal is then to prove that $\forall n$, $P(n)$ is true. This consists of two steps:

Base Step: Prove $P(1)$.

Inductive Step: $\forall k$, show that $P(k) \Rightarrow P(k+1)$.

Remark. This of course assumes that we have some sort of "guess" as to what $P(n)$ is. One method to find this, is by **inductive induction**, which essentially consists of guessing empirically.

▶ Sum of the first n integers

Conjecture 1.1. *We want to find an equation for the sum $1 + 2 + \cdots + n$. We begin by forming a conjecture via inductive induction:*

$$\begin{aligned} 1 &= 1 \\ 1+2 &= 3 \\ 1+2+3 &= 6 \\ 1+2+3+4 &= 10 \end{aligned}$$

We then see that a reasonable conjecture for the sum of the first n integers is

$$P(n) = \frac{n(n+1)}{2} = \binom{n+1}{2} \tag{1.2}$$

Proof. We proceed by induction.

- <u>Base Step:</u> $P(1) = \frac{1(1+1)}{2} = 1$
- <u>Inductive Step:</u> Assume that $P(k) = 1+2+\cdots+k = \frac{k(k+1)}{2}$. Now, given this assumption (sometimes known as the "inductive hypothesis"), we need to show that our conjecture holds for $P(k+1)$ i.e., that $P(k+1) = \frac{(k+1)(k+2)}{2}$. We proceed as follows:

$$\begin{aligned} P(k+1) &= 1 + 2 + \cdots + k + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \qquad \text{given our inductive hypothesis} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

□

Note that another way of obtaining our conjecture is to write:

$$\begin{aligned}1+2+\cdots+n&=s\\ n+(n-1)+\cdots+1&=s\end{aligned}$$

We can then add the two equations together with each lined up term to obtain:

$$\begin{aligned}(n+1)+(n+1)+\cdots+(n+1)&=2s\\ \frac{n(n+1)}{2}&=s\end{aligned}$$

Remark 1.3. Often times, there is no way around employing inductive induction (as we'll see in the next example). However, this is not the case in most applications of mathematical induction.

▶ Sum of the first n cubes

Conjecture 1.4. *This time, we want to find an equation for the sum $1^3+2^3+\cdots+n^3$. We again form a conjecture via inductive induction:*

$$\begin{aligned}1^3&=1\\ 1^3+2^3&=9\\ 1^3+2^3+3^3&=36\\ 1^3+2^3+3^3+4^3&=100\end{aligned}$$

We now conjecture that

$$P(n)=\frac{n^2(n+1)^2}{4} \tag{1.5}$$

While this may appear opaque, one simply needs to revisit our empirical results for the sum of the first n integers (on the previous page) to see that the sum of the first n cubes appears to be equal to the square of the sum of the first n integers.

Proof. We proceed by induction.

- Base Step: $P(1)=\frac{1^2(1+1)^2}{4}=1$s
- Inductive Step: Assume that $P(k)=1^3+2^3+\cdots+k^3=\frac{k^2(k+1)^2}{4}$. Now, given this assumption, we need to show that our conjecture holds for $P(k+1)$ i.e., that $P(k+1)=\frac{(k+1)^2(k+2)^2}{4}$. We proceed as follows:

$$\begin{aligned}P(k+1)&=1^3+2^3+\cdots+k^3+(k+1)^3\\ &=\frac{k^2(k+1)^2}{4}+(k+1)^3 &&\text{given our inductive hypothesis}\\ &=(k+1)^2\left(\frac{n^2}{4}+(n+1)\right)\\ &=\frac{(n+1)^2(n+2)^2}{4}\end{aligned}$$

□

▶ Helly's Theorem

Prior to the statement of the theorem, recall that $\mathbb{R}^d = \{(x_1, \ldots, x_d)\big|x_i \in \mathbb{R}\}$. Also recall that $X \subseteq \mathbb{R}^d$ is convex if for every $a, b \in X$, we have $[a, b] \subseteq X$. Now, we proceed to the statement of the theorem.

Theorem 1.6 (**Helly's Theorem**)**.** *Let $X_1, \ldots, X_n \subseteq \mathbb{R}^d$ be non-empty and convex s.t. every $(d+1)$ of them have non-empty intersection. Then, $X_1 \cap X_2 \cap \cdots \cap X_n \neq \varnothing$.*

Proof. We'll prove the theorem for $d = 1$, i.e., the real number line. We only prove the case when the sets are open intervals (which is almost the full generality). Let $I_1, I_2, \ldots, I_n$ be open intervals on $\mathbb{R}$.

$P(1)$ and $P(2)$ are obvious.

We seek to prove $P(3)$ by contradiction. Suppose that every $(d+1) = 2$ of our open intervals I have non-empty intersection but $I_1 \cap I_2 \cap I_3 = \varnothing$. Now, note that:

$$I_1 \cap I_2 \cap I_3 = (I_1 \cap I_2) \cap I_3 \tag{1.7}$$

Thus, for this expression to be empty, I_3 must lie either completely to the left of $(I_1 \cap I_2)$ or completely to the right of it. However, the former implies that $I_3 \cap (I_1 \cap I_2) = \varnothing$. This, contradicts our initial condition that every two non-empty convex sets must have non-empty intersection.

Now, consider $P(k)$ and $P(k+1)$. Before we begin, we use a trick by replacing the collection $I_1, I_2, \ldots, I_k, I_{k+1}$ with $I_1, I_2, \ldots, I_{k-1}, (I_k \cap I_{k+1})$. We need to check now that $I_i \cap I_k \cap I_{k+1} \neq \varnothing \ \forall i < k$. BUT, we've already proved $P(3)$! So, certainly the desired statement holds, as required. □

Remark. For higher dimensions, while the problem may be harder to visualize, the inductive step generalizes straightforwardly. The base step in the proof above requires another result from the convex geometry (Radon's Theorem) that we do not do here.

▶ Strong Induction

To prove a statement by **strong induction** (sometimes referred to as **complete induction**), we only have a single step to prove:

* Inductive Step: $\forall k, \Big(P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \Rightarrow P(k)\Big)$.

Remark. Note that we don't require a base step, since for $k = 1$, the premise here is always true, and we obtain $P(1)$ automatically.

Lecture 2 (Wednesday, September 28)

▶ Strong Induction (Review)

Recall that to prove something via strong induction, we only need to show that

$$\Big(P(1) \wedge P(2) \wedge \cdots \wedge P(k-1)\Big) \Rightarrow P(k) \tag{2.1}$$

Similarly, we can show

$$(\forall x < k), P(x) \Rightarrow P(k) \tag{2.2}$$

▶ Fundamental Theorem of Arithmetic

Theorem 2.3 (**Fundamental Theorem of Arithmetic**)**.** *Let $n \in \mathbb{N}$. Then, $\forall n \geq 1$, we can find a unique* **prime factorization (pf)** *of n. I.e., we can find prime numbers $p_1, p_2, \ldots, p_z$ and natural numbers $d_1, d_2, \ldots, d_z$ such that*

$$n = p_1^{d_1} \cdot p_2^{d_2} \cdot \cdots \cdot p_z^{d_z}, \tag{2.4}$$

and they are uniquely defined, up to a permutation.

Note that, to prove this theorem, we'll need to prove both *existence* and *uniqueness*. We prove existence below.

Proof. We need to show:

$$P(n): \ n \text{ has a prime factorization.}$$

We proceed by cases and strong induction.

Case 1: n is prime. So we can simply write $n = n$, and we're done.
Case 2: n is composite. In this case, we can write $n = m \cdot k$ for $m, k \in \mathbb{N}$ where $1 < m, k < n$. Then, we take the prime factorizations of k and m, by strong induction, and multiply them. Thus, we have shown that n must have a prime factorization. □

We take note that, had we used "regular" induction as opposed to strong induction, we would not have been able to perform our proof in this manner, as the factorization of $(n-1)$ does not help us to factorize n.

For those of us who are more on the computer-science side of things, the last step may look a lot like recursion, and it is! In reality,

$$\text{Recursion} \equiv \text{Induction} \tag{2.5}$$

In pseudo-code, the factorization would appear as follows:

Algorithm 1 Prime factorization pseudocode

```
procedure F($n$: non-negative integer)
    if $n$ is prime then
        return $n$
    else
        $n = m \cdot k$, $1 < m, k < n$
        return $F(m) \cdot F(n)$
    end if
end procedure
```

▶ Well-ordering Principle

Principle 2.6 (Well-ordering Principle). *Every non-empty set of positive integers has a minimal element. We say that such a set is **well-ordered**.*

Remark. Note that we use the term "minimal element" and not "least element." For some set, say X, $y \in X$ is a **minimal element** if y is not larger than any other element. Either $y \leq x \ \forall x \in X$ or x and y are incomparable. A **least element**, say $z \in X$, is one such that $z \leq x \ \forall x \in X$. This difference in incomparability is one we'll visit later when we discuss partially ordered sets. For now, it is immaterial.

To prove the well-ordering principle, we simply employ mathematical induction.

Proof. Let $X \subseteq \mathbb{N}$ with $X \neq \varnothing$. Also let $X_n = X \cap \{1, \ldots, n\}$. It suffices to show

$$P(n): \ X_n = \varnothing \text{ or } X_n \neq \varnothing \text{ and has a least element} \tag{2.7}$$

Note that since $X \neq \varnothing$, $X_n \neq \varnothing$ for sufficiently large n.

Now, we proceed by induction.

Base step: $P(1)$ is obvious.

Inductive step: Assume $P(n-1)$ is true. Then, we can assume $X_n \neq \varnothing$ without loss of generality. We procced by cases:

Case 1: $X_{n-1} = \varnothing \Rightarrow X_n = \{n\}$ is obvious.

Case 2: $X_{n-1} \neq \varnothing$. Then, we know that X_{n-1} must have a minimal element, say a, by our inductive hypothesis. So, $a \leq n-1$. Clearly then, $a < n$, and so a must be the minimal element of X_n as well. □

Theorem 2.8. *The well-ordering principle implies the principle of strong induction.*

Proof. Fix P such that (2.2) holds. Let X be the set of counterexamples, i.e., let $X = \{n \big| \neg P(n)\}$ (recall that $\neg$ is the logical not operator). Thus, to reach the desired conclusion, it suffices to show that $X = \varnothing$. We proceed by contradiction:

Assume $X \neq \varnothing$. Since $\mathbb{N}$ is well-ordered, there exists $n \in X$ such that n is minimal. I.e., n is our *minimal counterexample.* BUT, this implies that everything smaller than n doesn't violate P. In other words, $P(1), P(2), \ldots, P(n-1)$ are true. BUT, this contradicts the inductive step of mathematical induction (2.2)! And so, we're done. □

Remark 2.9. The method we employed of "taking a minimal counterexample" is quite useful, as we'll see in the following example. Also, we note that since regular induction is a weaker principle, Theorem 2.8 applies to it as well.

▶ Finger-pointing Game

Proposition 2.10. *Consider a game where we start with a room with a finite number, say n, of people. Now, each person must point at* exactly one other *person in the room. It then follows that there must exist a finite "pointing cycle" in the room. I.e., person 1 points to person 2 who points to person 3 … who points to person m who points to person 1 with $m \leq n$.*

Proof. Consider the game with a room of n people. We need to show there exists a finite cycle within the room. We proceed by contradiction by taking a minimal counterexample.

Suppose that there is no such finite cycle in our room of n people. Now, for the sake of demonstration suppose that in this room we have a person named Alice. Alice is pointing at Bob, and anybody who is pointing at Alice (though it isn't necessary that there actually be anyone pointing at Alice, it is OK) is named Charlie.

Since this is a minimal counterexample, we know that there must exist a finite cycle in any room with $n-1$ people. Suppose then, that we tell Alice to leave the room and the Charlies (who may or may not exist), should now all point to Bob. Then, a finite cycle must exist in the room in one of two ways:

Case 1: A finite cycle exists that does not involve the Charlie's or Bob. But, this means that a finite cycle must have existed before Alice left the room, a contradiction to our counterexample.

Case 2: A finite cycle now exists that includes either the Charlie's or Bob. But, this implies that a finite cycle must have existed when Alice was in the room, but that the cycle was longer by just one chain (by detouring through Alice), also a contradiction to our counterexample. □

Remark 2.11. It is again very easy to see this particular statement directly. It is not the case, however, in more sophisticated applications.

▶ Linear Orderings (Total Orderings)

Definition 2.12. Using the **axiomatic method**, we say that a ground set S is **linearly (totally) ordered** if, $\forall a, b, c \in S$, S follows these axioms:

1. Reflexivity: $a \leq a$
2. Anti-symmetry: $(a \leq b \wedge b \leq a) \Rightarrow a = b$
3. Transitivity: $(a \leq b \wedge b \leq c) \Rightarrow a \leq c$
4. Totality: $(a \leq b \vee b \leq a)$

Notation 2.13. Before we continue with examples of linearly ordered sets and non-linearly ordered sets, we make a brief aside regarding notation. We say that $m|n$ if m divides n evenly. I.e., $(a = \frac{n}{m}) \in \mathbb{Z}$.

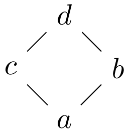
Examples 2.14. We consider the following sets and determine whether they are linearly ordered or not.

1. $\mathbb{N}$: ✓
2. $\mathbb{Z}$: ✓
3. $\mathbb{Q}$: ✓
4. $\mathbb{C}$: The complex numbers do NOT form a linearly ordered set, as the set fails totality. E.g., how would one compare $(3 + 6i)$ and $(7 + 2i)$?
5. $\mathbb{N}$ ordered by divisibility, i.e., $x_1 \leq x_2$ is declared to be true iff $x_1|x_2$: This set is NOT linearly ordered as it fails totality. E.g., how would one compare 4 and 5?

Definition 2.15. A set that satisfies reflexivity, anti-symmetry, and transitivity (but not necessarily totality) is called a **partially ordered set** (a.k.a., a **poset**).

Remark 2.16. Take note, then, that, while the fourth and fifth sets from **Examples 2.13** are not totally ordered, they *are* partially ordered.

We can begin with an example of a partially ordered set (poset):



This defines $a \leq b$, $a \leq c$, $a \leq d$, $c \leq d$, and $b \leq d$. The elements c and b are incomparable.

▶ Linear Extension

It turns out that it is possible to extend any poset to a linear order. To prove this in general requires the axiom of choice (it seems to be weaker than AC, though). However, we can use reverse induction to prove this in the finite case.

Usual induction relies on the existence of a least element; the inductive step reduces a problem to a smaller one (or, in case of strong induction, to several smaller ones). Reverse induction relies on the existence of a maximum element in a *finite* set.

Proposition 3.1. *Let $(S, \preceq)$ be a partially ordered set. Then there exists some linear order $\leq$ such that $a \preceq b$ implies $a \leq b$. We say that $(S, \leq)$ is a* linear extension *of $(S, \preceq)$.*

Proof (finite case). Let $(S, \preceq)$ be a finite poset. Define the cardinality of $\preceq$ to be the number of pairs of elements that may be compared, $|\preceq|$. For example, in the above example of a poset, $|\preceq| = 9$. Four between the distinct elements represented by the edges of the graph, the pair (a, d), and since each element may be compared to itself, four more. In general for a finite set,

$$|\preceq| \leq |S|^2,$$

so $|\preceq|$ is finite, and we may use reverse induction.

Suppose $|\preceq| = n$, and that $(S, \preceq)$ is not already a linear order. Then, there exists two incomparable elements, $a, b \in S$. Define $\preceq'$ by (pardon the abuse of notation)

$$\preceq' = \preceq \cup \{c \preceq' d \,|\, c \preceq a, b \preceq d\}.$$

That is, take any $c \preceq a$ and $d \succeq b$. Define $\preceq'$ such that $c \preceq' d$ in addition to preserving the original order. In particular, c may equal a and d may equal b, so we also have $a \preceq b$.

We claim that $\preceq'$ is an order extending $\preceq$ such that $|\preceq| < |\preceq'|$. Therefore, we can apply reverse induction, and $\preceq'$ may be extended to a linear order $\leq$, which then also extends $\preceq$.

It's easy to see that $|\preceq| < |\preceq'|$ since $\preceq'$ compares not only everything $\preceq$ can, but also a and b, so $|\preceq| < |\preceq'|$. All that's left to do is to show that $\preceq'$ is an order.

1. Because $\preceq$ is reflexive, so is $\preceq'$.
2. Suppose $c \preceq' d$ and $d \preceq' c$. If (c, d) and (d, c) are comparable under $\preceq$, then $\preceq'$ is defined to preserve their order; $c \preceq' d$ and $d \preceq' c$ implies $c \preceq d$ and $d \preceq c$. So, $c = d$.

If neither (c,d) nor (d,c) are comparable under $\preceq$, then $c \preceq' d$ implies $c \preceq a$ and $b \preceq d$. Likewise, $d \preceq' c$ implies $d \preceq a$ and $b \preceq c$. So,

$$c \preceq a \preceq b \preceq c$$

implies $a = b = c$. Similarly, $a = b = d$, so $c = d$.
Without loss of generality, suppose (c,d) is comparable, but (d,c) is not. The latter then implies the existence of incomparable elements $a, b \in S$ such that $d \preceq a$ and $b \preceq c$. The former implies $c \preceq d$. But this then implies $b \preceq c \preceq d \preceq a$, a contradiction to the assumption that a and b are incomparable under $\preceq$. Therefore, in all possible cases, we have shown $c \preceq' d$ and $d \preceq' c$ implies $c = d$, proving anti-symmetry.

3. Suppose $c \preceq' d$ and $d \preceq' e$. Then either c, d, e are already pairwise comparable under $\preceq$, in which case $c \preceq d$ and $d \preceq e$ implies $c \preceq e$ implies $c \preceq' e$. Or, one of the pair (c,d) or (d,e) are not comparable under $\preceq$. This implies that either $d \preceq a$ or $b \preceq d$. It follows that one of the pairs must be comparable. So, it is the case that

$$[(c \preceq d) \wedge (d \preceq a) \wedge (b \preceq e)] \vee [(c \preceq a) \wedge (b \preceq d) \wedge (d \preceq e)].$$

These two cases both imply $c \preceq' e$.

This completes the proof. □

▶ Transfinite Induction

Recall that we can prove strong induction from the well-ordering principle; we relied on being able to find a *minimal counterexample.* It is this property of natural numbers that allows strong induction to hold. As an example of a false proof is this:

False Theorem 3.2. *Every integer $n \in \mathbb{Z}$ is greater than or equal to 10.*

Proof. We use strong induction. Suppose $n - 1 \geq 10$, then $n \geq 10$. By strong induction, $n \geq 10$ for all $n \in \mathbb{Z}$. Of course, this is wrong; we can't apply strong induction here because $\mathbb{Z}$ is not well-ordered, unlike $\mathbb{N}$. □

Now, why does the same proof not prove that $n \geq 10$ for all $n \in \mathbb{N}$? Because it might be the case that $n - 1$ does not exist. So, we need a separate case for this; this turns out to be equivalent to the base case in usual induction, $n = 0$. That doesn't hold, so this theorem is false for both $\mathbb{N}$ and $\mathbb{Z}$.

Definition 3.3. A linear order $(S, \leq)$ is well-ordered if every nonempty subset has a minimal element.

The well-orderedness of $\mathbb{N}$ is the only thing we needed to prove strong induction, so the proof from Lecture 2 also proves that any well-ordered set permits induction.

Proposition 3.4 (Transfinite Induction)**.** *Let S be a well-ordered set and $P(x), x \in S$ be any statement. Then,*

$$(\forall y < x)(P(y) \to P(x)) \implies \forall x P(x).$$

We call this transfinite induction.

Examples of sets that are not well-ordered include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and even $\mathbb{Q}_+$; we can't apply transfinite induction to these sets.

However, if we're given a well-ordered set S, any nonempty subset $T \subset S$ is also well-ordered. For example, $\mathbb{N}$ and $X = \{2, 4, 6, 8, \dots\}$ are both well-ordered. But notice that these are order-isomorphic. One says that *up to isomorphism*, $\mathbb{N}$ and X are equal. In fact, we give the equivalence class of posets isomorphic to $\mathbb{N}$ a name, ω. Similarly, we let n denote the equivalence class of posets isomorphic to $\{1, \dots, n\}$. ω and n are our first examples of *ordinal numbers*, that is equivalence classes of well-ordered sets up to isomorphism.

▶ Sums of Well-Ordered Sets

We can construct a new well-ordered set by adding a single point to ω, so that it is greater than everything else. We can call this $\omega + 1$. Continuing, we can construct:

$$\begin{aligned}
&\omega\\
&\omega + 1\\
&\omega + 2\\
&\vdots\\
&\omega + \omega = \omega \times 2\\
&\omega \times 3\\
&\vdots\\
&\omega \times \omega\\
&\vdots
\end{aligned}$$

In general, given two well-ordered sets S, T, we can construct a new well-ordered set, $S + T$, where the ground set is $S \sqcup T$ (or $S \dot{\cup} T$, the disjoint union), the relation between two elements of S or T are preserved, and $s \leq t$ for all $s \in S$ and $t \in T$.

It's easy to see that $S + T$ is well-ordered. If $\varnothing \neq X \subset S + T$, either $X \cap S \neq \varnothing$, in which case the minimal element of $X \cap S$ is the minimal element of X, or $X \cap S = \varnothing$, in which case $X \subset T$. Then, the minimal element of X in T is the minimal element of X in $S + T$.

Remark 3.5. Notice that $+$ is not commutative here. The order $2 + \omega$ is distinct from $\omega + 2$. In fact, $2 + \omega = \omega$. However, by inspection, we can see that $+$ is associative.

Lecture 4 (Monday, October 3)

Recall that an *ordinal* is an equivalence class of well-ordered sets that are order-isomorphic. Last time, we had examples of

$$n, \quad \omega, \quad \omega + n.$$

In general, if we are given two well-ordered sets, S and T, we can construct the well-ordered set $S + T$. We can also construct the well-ordered set $S \times T$.

▶ Products of Well-Ordered Sets

Let S and T be two well-ordered sets. We define the set of $S \times T$ to be $S \times T$ in the usual sense of the product, and we also define the order $\leq$ between two points $(s_1, t_1), (s_2, t_2) \in S \times T$ to be

$$(s_1, t_1) \leq (s_2, t_2) \text{ if and only if } (t_1 < t_2) \vee [(t_1 = t_2) \wedge (s_1 \leq s_2)].$$

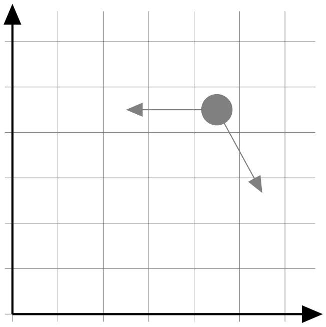
That is, we compare the second coordinate first; if they are equal, then we compare the first coordinate. We call this the *antilexicographic ordering* on $S \times T$. It's kind of like looking up a word in the dictionary, except that we look up a word by its last letter first. An example of the product of two well-ordered sets is $\omega \times 2$.

Theorem 4.1. *If S, T are well-ordered, then $S \times T$ is well-ordered.*

Proof. Let $X \subset S \times T$ be nonempty. Because T is well-ordered, we can consider the subset X' of X containing all elements with the least second coordinate t_0. And because S is well-ordered, we can find the smallest first coordinate s_0 in X'. It's easy to check that (s_0, t_0) is the least element of X, so $S \times T$ is well-ordered. □

Exercise 4.2. To prove that two well-ordered sets S, T are equal, we need to construct an order-preserving bijection $f : S \to T$ such that its inverse, $f^{-1} : T \to S$ is order-preserving. Check that $\omega + \omega = \omega \times 2$. Check that $\omega \times 2 \neq 2 \times \omega$.

The product well-ordered sets gives us an example of *double induction*, or *transfinite induction* on $\omega \times \omega$. Consider the following chessboard, going off to infinity along the positive x and y axes.



Imagine a game piece that, at every turn, can only move to the left or down and to the right (through any number of squares in each case). We claim that no matter where the piece starts, after a finite number of moves, it will become stuck at the origin. The proof is just an application of transfinite induction.

First, we can give the chessboard an order isomorphic to $\omega \times \omega$. Once we do this, we realize that the two allowable moves (where defined) are strictly decreasing. This lets us use transfinite induction: assume that a piece starting at a position less than x will land on the origin after a finite number of moves. If it starts on x, then after a single move, it will be on a position less than x, so after a finite number of moves, a piece starting on x will land on the origin.

Definition 4.3. Let $\omega^\omega = \omega + \omega^2 + \omega^3 + \cdots + \omega^n + \cdots$. We can also get $\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$ in this way.

We end our brief foray into this beautiful theory with three facts:

Fact 4.4. *Ordinals are themselves well-ordered.*

Fact 4.5. *Every nonempty set can be well-ordered if you assume the axiom of choice.*

Fact 4.6. *Any countable ordinal can be order-embedded into $\mathbb{R}$.*

▶ Number Theory

The subject of the next block of the course is number theory.

Recall the statement of the Fundamental Theorem of Arithmetic:

Theorem 4.7 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 1$ has a unique prime factorization $n = p_1^{t_1} \cdots p_d^{t_d}$, where $t_i > 0$ and $p_1 < \cdots < p_d$.*

In Lecture 2, we proved the existence claim by strong induction on n. Now we prove uniqueness, modulo the truth of a "main lemma."

Lemma 4.8 (Main Lemma)**.** *If p is a prime and $p|a_1 \cdots a_n$, then $p|a_i$ for some i.*

By the principle of induction, to prove the lemma it suffices to show that $p|ab$ implies $p|a$ or $p|b$. The strategy for applying this special case to prove the statement for arbitrary n is similar to the strategy used in the proof of Helly's Theorem (Lecture 1).

We will prove the lemma in a later lecture. In the meantime, the student is encouraged to attempt the proof by himself and discover that it requires ideas beyond those we've so far discussed. Let us now apply the lemma to the proof of the uniqueness claim of the Fundamental Theorem of Arithmetic.

Uniqueness of prime factorization. Suppose for contradiction that n factors into primes in two distinct ways $n = p_1^{t_1} \cdots p_d^{t_d} = q_1^{s_1} \cdots q_e^{s_e}$. Without loss of generality, $p_1, \ldots, p_d$ are pairwise different from $q_1, \ldots, q_e$. (If any p_i equals any q_j, then we simply cancel those factors, and the problem is reduced to the uniqueness claim for smaller n). Since $p_1|q_1^{s_1} \cdots q_e^{s_e}$, the lemma says that p_1 must divide at least one of $q_1, \ldots, q_e$, which is impossible since $p_1, q_1, \ldots, q_e$ are primes and p_1 is not equal to any q_i □