Lecture 4: Mathematical Induction

Recall that if we want to prove some assertion for all positive integers, and \( A(n) \) denotes the truth of this assertion for the particular positive integer \( n \), then induction says:

(i) \( A(1) \)
(ii) \( A(n) \Rightarrow A(n+1) \) (for each \( n \in \mathbb{N} \))

\[ \Rightarrow \quad A(n) \text{ for every } n \in \mathbb{N}. \]

We begin with a really important consequence of induction:

**The Well-Ordering Principle:** Every nonempty set \( T \subseteq \mathbb{N} \) contains a smallest element. (i.e. \( \inf(T) \in T \))

**Proof:** Suppose \( T \) doesn’t have a smallest element (\( \inf(T) \notin T \)).

Write \( S := \{ k \in \mathbb{N} \mid k \leq t \text{ for every } t \in T \} \), and let \( A(n) \) mean \( n \in S \).

Clearly \( 1 \notin T \) (otherwise it’s smallest), so \( A(1) \) is true.

Suppose \( A(n) \) holds. If \( A(n+1) \) fails, then \( n+1 \notin T \) for some \( t \in T \).

Since \( T \) has no smallest element, \( \exists t' \in T \) with \( t' < t \), hence \( t' < n+1 \). But \( n, t' \in \mathbb{N} \), and so \( t' \leq n \), contradicting \( A(n) \).

So \( A(n) \Rightarrow A(n+1) \), making \( S \) an inductive set hence \( S = \mathbb{N} \), a contradiction since \( T \) is nonempty.

This allows us, in turn, to prove “improved” forms of induction:

(i) \( A(1) \)
(ii) \( A(k) \text{ for all } k \leq n \Rightarrow A(n+1) \) (for any \( n \in \mathbb{N} \))

**Proof:** Suppose \( T := \{ n \in \mathbb{N} \mid A(n) \text{ false} \} \) is nonempty. Then by the WOP, \( T \) has a least element \( t_0 \). For any \( n < t_0 \), \( n \notin T \)
that is, $A(n)$ is true. Now consider the following 2 cases:

t₀ = 1: impossible, as it contradicts (i)

t₀ > 1: by (ii), $A(t₀)$ is thus true, contradicting $t₀ ∈ T$.

Therefore our supposition was absurd, and $T$ is empty. □

there's an application:

Ex/ Define the Fibonacci series by $a₁ = 1$, $a₂ = 2$, $aₙ₊₁ = aₙ + aₙ₋₁$ (for $n ≥ 2$). Let "$A(n)$" mean $aₙ < qⁿ$, where $q = \frac{1+\sqrt{5}}{2}$ is the golden ratio. Clearly $A(1)$ holds, since $q > 1$. Suppose that $A(n)$, $A(n-1)$, ... all hold. Then $aₙ₊₁ = aₙ + aₙ₋₁ < qⁿ + qⁿ₋₁ = qⁿ₊₁$, so $A(n₊₁)$ holds. (The equality is false: it is because $q² = \frac{(1+\sqrt{5})²}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + q$ (now multiply by $qⁿ₋₁$).)

[Remark: In induction, you can always replace (i) by $A(n₀)$ and (ii) by $A(n) ⇔ A(n₊₁)$ for $n₀ ≥ n₀$. The conclusion is then that $A(n)$ holds for all $n ≥ n₀$. Hence $n₀$ could be 0 or bigger than 1.]

Another application of the WOP (used in Lecture 3 !) is:

Theorem: If $p, r ∈ R$ and $p < r$, then $∃ q ∈ Q$ with $p < q < r$.

Proof: Since $r - p ∈ R^+$, the Archimedean property of $R$ guarantees an $n ∈ N$ such that $n(r - p) > 1$ ($⇒ n(r - p) > 1 =⇒ n(r + 1) < nr$).
By the WOP, \( S := \{ k \in \mathbb{P} \mid k > np \} \) has a least element \( s_0 \).
Hence \( s_0 > np \), but \( s_0 - 1 \leq np \), which gives
\[
np < s_0 \leq np + 1 < nr
\]
\[
p < \frac{s_0}{n} < r \quad \text{, done.} \]

One more (a bit long, you can skip if not interested):

Theorem (Euclid): There are infinitely many prime numbers.

Proof: Suppose \( S = \{ n \in \mathbb{P} \mid \text{n has no prime factorization} \} \neq \emptyset \).
It has a least element \( N \), by WOP. This \( N \) can't be prime, b/c then it is its own prime factorization! So \( N \) has a divisor \( M > 1 \), i.e. \( N = ML \) for \( M, L \in \mathbb{P} \).
Put \( M, L < N \Rightarrow M, L \notin S \Rightarrow M, L \)
have prime factorization, \( M_{1} ... M_{k}, L_{1} ... L_{k} \Rightarrow \)
\( N = M_{1} ... M_{k} L_{1} ... L_{k} \) is a prime factorization \( \Rightarrow N \notin S \neq \emptyset \).
\( s_0 = \emptyset \), i.e. every positive integer has a prime factorization.

Now suppose there are finitely many primes \( \{ p_1, p_2, ..., p_m \} \).
Let \( Q := 1 + p_1 p_2 ... p_m \). It has a prime factorization
\( Q = p_1^{a_1} p_2^{a_2} ... p_m^{a_m} \), with at least one of the \( a_i > 0 \).
That is, \( p_i \) divides \( Q \); since it also divides \( p_1 p_2 ... p_m \),
it divides \( Q - p_1 p_2 ... p_m = 1 \), a contradiction. \( \square \)
Final application of induction: recall \( \binom{n}{k} := \frac{n!}{(n-k)!k!} = \frac{n(n-1)...(n-k+1)}{k(k-1)...1} \)

with conventions \( \binom{0}{0} = 1, \binom{n}{1} = 0 = \binom{n}{n+1} \). We'll need the

Pascal's triangle identity: \( \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \).

(That doesn't require induction to check. Just write
\[
\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{(n-k)!k!} + \frac{n!}{(n+1-k)!k-1)!} = \left( \frac{1}{k} + \frac{1}{n+1-k} \right) \frac{n!}{(n+1-k)!k!} \frac{n!}{(n-k)!k-1)!} = \frac{n+1}{k(n+1-k)} \frac{n!}{(n-k)!k-1)!} \frac{n+1}{(n+1-k)!k!} = \binom{n+1}{k}.
\]

(You'll use this in Problem 12 on p. 45 to show what amounts to the statement that \( e < 3 \).

Binomial Theorem: \( (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \), \( a, b \in \mathbb{R} \).

Proof: Well, "\( A(1) \)" is clearly true:
\[ (a+b)^1 = a+b = (\binom{1}{0} a + \binom{1}{1} b). \]

"\( A(n) = A(n+1) \)":
\[
(a+b)^{n+1} = (a+b) \cdot (a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} = \sum_{k=0}^{n+1} \left[ \binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n+1-k} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
\]

P.S. Have a look at the triangle & Cauchy–Schwarz inequalities on pp. 42–43. (We won't use them right now, though.)