Tuesday: Induction

Mathematical Induction [3.1, 3.2]

Mathematical Induction is a process we may use to prove that some statement P_n is true for all natural numbers n.

Example 1. *Find* $|\mathcal{P}(\{1,2,\dots,n\})|$ *for the first few values of* $n = 1,2,3,\dots$ *and form a conjecture on what the size of this set is for arbitrary* n.

Example 2. *Calculate* n^2+n+41 *for the first few values of* $n = 1,2,3,\dots$ *and form a conjecture on whether or not* n^2+n+41 *is prime for arbitrary* n.

Induction is the process of inferring that something will be true in the future because it has always been true so far. While this idea may be the best bet for scientific theories, the second example above shows it cannot be used to prove things mathematically.

A proof by mathematical induction, showing that the statement P_n is true for all $n \in \mathbb{N}$, must establish that

- P_1 is true (this is called the *base case*); and
- for any $n \in \mathbb{N}$, if P_n is true then P_{n+1} is true (this is called the *inductive step*, and the hypothesis P_n of this implication is called the *inductive hypothesis*).

Example 3. *Prove by induction that if* $n \in \mathbb{N}$ *then*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof. Let P_n be the statement $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Base case: when $n=1$ we have $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$.

Inductive step: Let $n \in \mathbb{N}$ and suppose that P_n is true. Then

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1) \\ &= \frac{n(n+1)}{2} + n + 1 && \text{(by inductive hypothesis)} \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

So $\sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$, so P_{n+1} is true.

Hence, by induction, P_n is true for all $n \in \mathbb{N}$. $\square$

Example 4. *Prove by induction that if $n \in \mathbb{N}$ and A is a set with n elements then $\mathcal{P}(A)$ has 2^n elements.*

Solution. See 3.2.1 and 2.5.7. $\square$

Example 5. *Find a formula for $\sum_{i=1}^{n} i^2$ and show that your formula holds for all $n \in \mathbb{N}$.*

Wednesday: Further examples of induction

For $m, n \in \mathbb{Z}$, we say that m *divides* n, written $m \mid n$, if there is some $a \in \mathbb{Z}$ with $n = ma$. For example, n is even if $2 \mid n$.

Important: don't mix "m divides n", which is a statement, with "m divided by n" which is a number. [The distinction is like the distinction between the statement "Mary is a mother" and the person "Mary's mother".]

Example 6. *Prove that for all $n \in \mathbb{N}$, $6 \mid n^3 - n$.*

Example 7. *Prove that for all $n \in \mathbb{N}$, $3 \mid 8^n - 5^n$.*

Example 8. *Show that for all $n \in \mathbb{N}$, $n < 2^n$.*

Sometimes we wish to show that P_n is true for all $n \geq 2$ or for all $n \geq 17$ or something. In this case we make the base case $n = 2$ or $n = 17$ instead of $n = 1$.

Example 9. *Suppose a post shop only stocks postage stamps in two denominations: 30 cents and 80 cents. Suppose also that all postage rates are multiples of 10 cents. Show that for any postage rate over $1.40 we can buy stamps for that rate.*

Proof. We are being asked to prove that for every $n \in \mathbb{N}$ with $n \geq 14$ there exist integers $m, k \geq 0$ with $3m + 8k = n$. We prove this by induction on n. So let P_n be the statement that there exist $m, k \in \mathbb{Z}$ with $m, k \geq 0$ and $3m + 8k = n$

Base case: The base case is $n = 14$. P_14 is true because $14 = 2 \cdot 3 + 1 \cdot 8$.

Inductive step: Suppose $n \geq 14$ and P_n is true. Then there exist $m, k \geq 0$ so that $n = 3m+8k$. If $k > 0$, put $k' = k - 1$ and $m' = m + 3$: then $3m' + 8k' = 3(m + 3) + 8(k - 1) = 3m + 8k + 9 - 8 = n + 1$ as required. If $k = 0$ and $m > 4$, put $k' = k+2$ and $m' = m-5$: then $3m'+8k' = 3(m-5)+8(k+2) = 3m + 8k - 15 + 16 = n + 1$, as required. So the only problem occurs if $k = 0$ and $m \leq 4$. But this cannot happen because then we would have $n = 3m + 8k \leq 12$, and we assumed that $n \geq 14$.

$\square$

Thursday: Complete Induction

Complete Induction [3.3]

In the examples considered so far we have deduced P_{n+1} from P_n. As an alternative, we may use *Complete Induction.* To prove by complete induction that P_n is true for all $n \in \mathbb{N}$, we have to prove

- P_1 is true; and
- if P_j is true for all $1 \le j < n$ then P_{n+1} is true.

Example 10. *Prove that every integer greater than 1 can be written as a product of (one or more) prime numbers.*

Example 11. *Prove that every natural number can be written as a sum of distinct powers of 2.*

Example 12. *Consider the following algorithm. We start with some number n. If $n = 1$, we stop. If $n = 2^k$ for some k, we replace our value of n with k. Otherwise we replace it with $n + 1$. For example, if we start with $n = 6$ we get the values 6, 7, 8, 3, 4, 2, 1. If we start with $n = 28$ we get 28, 29, 30, 31, 32, 5, 6, 7, 8, 3, 4, 2, 1.*

Prove that whatever natural number we start with, this algorithm will terminate in some finite number of steps.

Friday: Relations

Relations, ordered pairs and cartesian products

Consider the guests at a party: some of the people know each other, others do not. We could form the set of all pairs (x, y) such that x knows y's name. For example, if Mark and Sarah know each other, then we would include the pair $(\text{Mark}, \text{Sarah})$ in our set and also the pair $(\text{Sarah}, \text{Mark})$. Note that we are using round brackets $(,)$ rather than curly brackets $\{ , \}$ because the order of the elements in the pair matters. Although $\{1, 2\} = \{2, 1\}$, $(1, 2) \neq (2, 1)$. [Unfortunately, this means that we have two possible meanings for (x, y) when $x, y \in \mathbb{R}$: either the ordered pair of x and y, or the open interval of all z with $x < z < y$. We will try to make it clear which one we mean at any given time.]

Returning to the party example, note that we could have a situation where x knows y's name but y does not know x's name, for example if y is someone famous or x is someone forgetful.

Definition. *Let A and B be sets. The* cartesian product *of A and B, $A \times B$, is the set*

$$A \times B = \{ (a, b) : a \in A, b \in B \}.$$

Example 13. *Let $A = \{1, 2, 3\}$, $B = \{a, b\}$. Find $A \times A$, $A \times B$, $B \times A$ and $B \times B$.*

Definition. *Let A and B be sets. A* relation from A to B *is a subset of $A \times B$. A* relation on A *is a subset of $A \times A$.*

We often use *infix* notation for relations: in other words, if ρ is our relation, instead of writing $(x, y) \in \rho$ we write $x \,\rho\, y$, and instead of $(x, y) \notin \rho$ we write $x \not\rho\, y$. We often use the symbol $\sim$ for a relation on a set A.

Definition. *Let ρ be a relation on a set A. We say that ρ is*

- reflexive *if for all $a \in A$, $a \,\rho\, a$.*
- symmetric *if for all $a, b \in A$, if $a \,\rho\, b$ then $b \,\rho\, a$.*
- antisymmetric *if for all $a, b \in A$, if $a \,\rho\, b$ and $b \,\rho\, a$ then $a = b$.*
- transitive *if for all $a, b, c \in A$, if $a \,\rho\, b$ and $b \,\rho\, c$ then $a \,\rho\, c$.*

Example 14. *Let A be the set of people at a party. Let ρ, σ and τ be the following relations: $x \ \rho \ y$ if x knows y's name; $x \ \sigma \ y$ if x is older than y; and $x \ \tau \ y$ if x is taller than y. Which, if any, of these properties are ρ, σ and τ likely to have? Note that the definitions are a bit vague: is it possible for two different people to be the same age, or the same height? You will have to make some guesses about how well the people at the party know each other too.*

Example 15 (4.1.10). *Consider the following relations. Which, if any, of the four properties do these relations have?*

1. $A = \{ p : p \text{ is a person in Alaska } \}$, $x \sim y$ if x is at least as tall as y.
2. $A = \mathbb{N}$, $x \sim y$ if $x + y$ is even.
3. $A = \mathbb{N}$, $x \sim y$ if $x + y$ is odd.
4. $A = \mathcal{P}(\mathbb{N})$, $x \sim y$ if $x \subseteq y$.
5. $A = \mathbb{R}$, $x \sim y$ if $x = 2y$.
6. $A = \mathbb{R}$, $x \sim y$ if $x - y$ is rational.

Example 16. *Recall that for $m, n \in \mathbb{Z}$, $m \mid n$ if there is some $a \in \mathbb{Z}$ with $n = ma$. Show that $\mid$ is reflexive and transitive and not symmetric. Show that $\mid$ is not antisymmetric on $\mathbb{Z}$ but is antisymmetric on $\mathbb{N}$.*