Induction

Berkeley Math Circle
November 18, 2001

Ted Alper
Ted.Alper@stanford.edu

1 Introduction

1.1 Example (definition to follow)

Problem #1 Show that (for any integer $n > 1$):

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \ldots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n}$$

.

OK, you *could* prove this by breaking each term $\frac{1}{k \cdot k+1}$ down into $\frac{1}{k} - \frac{1}{k+1}$ and turning the left hand side into a telescoping sum. But *another* way to do this problem is to *first* show that the formula is true for the smallest possible value for n (that is, when $n = 2$, the two sides of the equation are identical) and *then* to show that, once we have confirmed the formula is ok for some number n, we can add $\frac{1}{n \cdot (n+1)}$ to both sides, do a little algebra on the right side, and obtain the formula:

$$\begin{aligned} \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \ldots + \frac{1}{(n-1) \cdot n} + \frac{1}{n \cdot (n+1)} &= \frac{n-1}{n} + \frac{1}{n \cdot (n+1)} \\ &= \frac{(n-1) \cdot (n+1) + 1}{n \cdot (n+1)} \\ &= \frac{n}{n+1} \end{aligned}$$

which is exactly the same formula, but applied to the number $n + 1$. Putting this together, means that we have shown the equation is true for all positive integers greater than 1. *Haven't we?*

1.2 The formal definition

> If k is an integer, and P is some property of integers (that is, for every integer n, $P(n)$ is a statement – meaning something that is either true or false – for instance, it could be the equation mentioned above). Then, if
>
> **"base case":** $P(k)$ is true and
>
> **"induction step":** *whenever* $P(n)$ is true, then $P(n+1)$ is also true.
>
> then $P(n)$ is true for all integers $n \geq k$.

The antecedent of the induction step, (the temporary assumption that $P(n)$ is true), is also called the *induction hypothesis*.

I like to think of induction as sort of like climbing a ladder. The base case is the bottom rung of the ladder and the induction step shows you how to climb from one rung to the next. If you know how to get to the bottom rung, and you know how to climb from one rung to the next, you can climb to every rung above the bottom one! Some people prefer a domino metaphor.

1.3 Some other examples

Problem #2 $2^n < n!$ for $n > 2$

Problem #3 If *any* square of a $2^n \times 2^n$ chessboard is removed, the remaining squares can be covered by L-triominoes. (That is, by blocks of size equal to three board squares, connected in an "L" shape). (This problem is often given where the square removed from the large chessboard is a corner square – but the proof works for any square.)

Problem #4 In a certain country, each town is connected to every other town by a (single) one-way road. Prove that there is one town from which you can drive to any other (you may need to stop in intermediate towns to do it).

Problem #5 With the same setup of towns and road as the previous problem, can you show that there is a town from which you can drive to any other, stopping in *at most* one intermediate town?

Problem #6 In the same setup as the previous two problems (but with the additional restriction that there are at least three towns) – can you show that, by changing the direction of at most one road, it is possible to get from ANY town to every other?

2 Variant forms of expressing induction

2.1 Strong induction versus weak induction

Sometimes the definition given above for induction is called "weak" induction – as contrasted with "strong induction", defined as follows:

> If k is an integer, and P is some property of integers, and
>
> **"base case":** $P(k)$ is true and
>
> **"induction step":** *whenever* $P(k), P(k+1), P(k+2), \ldots, P(n)$ are *all* true, then $P(n+1)$ is also true.
>
> then $P(n)$ is true for all integers $n \geq k$.

The difference is in what you need to assume in the induction step. For ordinary induction—in the ladder metaphor—you simply go from the rung you are on up to the next one. For strong induction, you need to know that all the rungs below the rung you are on are solid in order to step up. As a practical matter, both have the same logical strength when you apply them – since as you climb up the ladder from the bottom rung, you sweep

through all the intermediate rungs anyway. However, sometimes strong induction makes the proof of the induction step easier.

Problem #7 The proof that every integer greater than 1 may be written as the product of prime numbers is usually written with this form of induction.

Problem #8 (1991 USAMO) Show that for any fixed integer $n \geq 1$, the sequence:

$$2, 2^2, 2^{(2^2)}, 2^{\left(2^{(2^2)}\right)}, \ldots \pmod{n}$$

is eventually constant. [That is, the sequence is defined: $a_1 = 2$, $a_{i+1} = 2^{a_i}$. and you need to show that, for any positive integer n, the sequence $a_1 \bmod n$, $a_2 \bmod n, \ldots$ is eventually constant.]

This problem actually requires, in addition to induction, a little bit of number theory. Just because $a \equiv b \pmod{n}$ doesn't mean $2^a \equiv 2^b \pmod{n}$. What must be true of a and b in order for 2^a to be congruent to $2^b \bmod n$? (Hint: think of the Euler-Fermat theorem and $\phi(n)$.)

2.2 The method of descent

I hadn't intended to define this so formally, but here goes:

> If k is an integer, and P is some property of integers, if
>
> - whenever $P(n)$ is true for an integer $n > k$, then there must be some smaller integer j, $n > j \geq k$ for which $P(j)$ is true, and yet
> - $P(k)$ is *not* true
>
> then $P(n)$ must be *false* for all $n \geq k$.

Really, this is just the contrapositive of strong induction, applied to the negation of $P(n)$. In the language of the ladder metaphor, if you know you can't reach any rung without first reaching a lower rung, and you also know you can't reach the bottom rung, then you can't reach any rungs.

The above is often called *finite* descent, to distinguish it from the variant method known as *infinite* descent:

> If k is an integer, and P is some property of integers, if
>
> - whenever $P(n)$ is true for an integer $n > k$, there must be some smaller integer j, $n > j > k$ for which $P(j)$ is true
>
> then $P(n)$ must be *false* for all $n > k$.

That is, if there *were* an n for which $P(n)$ was true, you could construct a sequence $n > n_1 > n_2 > \ldots$ all of which would be greater than k – but for the integers, no such descending, but bounded below sequence is possible.

Problem #9 (Putnam, 1972) Show that, for all $n > 1$, n does not divide $2^n - 1$.

hint: here we are not using descent based on n, but on the prime factors of n. We will also need this much number theory (at least in my proof): $2^{p-1} \equiv 1 \bmod p$, and the smallest value m for which $2^m \equiv 1 \bmod p$ must be a factor of $p - 1$.

The classic example of infinite descent is in Fermat's proof that there are no positive integer solutions to $x^4 + y^4 = z^2$, or that every prime of the form $4p + 1$ is the sum of two squares. I'm including one of these along with an outline of the solution. **Problem #10** There are no positive integer solutions of $x^4 + y^4 = z^2$

SKETCH of proof: You need to know that every positive integer solution of $a^2 + b^2 = c^2$ where a,b and c are relatively prime can be expressed in terms of two relatively prime numbers m, and n where $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$. (Assuming b is the even one of a and b – one of them must be even)

So suppose you have a solution to $x^4 + y^4 = z^2$. Applying the above fact to the pythagorean triple x^2, y^2, z gives $x^2 = p^2 - q^2$, $y^2 = 2pq$, and $z = p^2 + q^2$. Since $2pq$ is a square, and p and q have no common factors. So one of p and q must be 2 times a square and the other is an odd square. And since one x, p, q themselves form a (relatively prime) pythagorean triple, we can see that there are r and s for which $x = r^2 - s^2$, $q = 2rs$, and $p = r^2 + s^2$. This means q is the one that is 2 times a square ($q = 2u^2$) and p is an odd square ($p = v^2$).

Now $q = 2u^2 = 2rs$, which means r and s are *themselves* perfect squares. Yet $r^2 + s^2 = p = v^2$ which means v^2 is expressible as the sum of fourth powers. Yet if we look at the construction of v, we see $v^2 < z^2$, which creates our infinite descent, a contradiction.

3 Related Topics

3.1 Recurrence relations/recursion & Induction

Recurrence relations and recursive definitions have a lot in common with induction – the value of a function at a higher value is defined in terms of its values at a smaller value.

Often a recursive construction will require an inductive proof of its correctness.

Example: $a_0 = 1$, $a_{n+1} = 2a_n + 1$, what is a closed form expression for a_n?

Then, show that the best solution to the $n - disk$ towers of Hanoi puzzle requires $2^n - 1$ steps.

A classic example of a recursive definition is that of the Fibonnaci numbers: they are defined as: $F_1 = F_2 = 1$ and, for $n \geq 1$, $F_{n+2} = F_{n+1} + F_n$.

Problem #11 Prove the following identity for Fibonacci numbers: for all $n \geq 1$:

$$F_1^2 + F_2^2 + \ldots + F_n^2 = F_n \cdot F_{n+1}$$

Problem #12 Prove that consecutive Fibonacci numbers are always relatively prime. (Hint: Try finite descent!)

Problem #13 For the Fibonacci numbers, show:

$$F_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \ldots$$

Problem #14 Show that every positive integer can be expressed *uniquely* as the sum of distinct, non-consecutive Fibonacci numbers (here, non-consecutive means that no two of the Fibonacci number in the sum are consecutive Fibonacci numbers).

3.2 Double Induction, etc.

Problem #15 (IMO, 1981) Let $1 \leq r \leq n$ and consider all subsets of r elements of the set $\{1, 2, \ldots, n\}$. Each of these subsets has a smallest member. Let $F(n, r)$ denote the arithmetic mean of these smallest members; prove that $F(n, r) = (n + 1)/(r + 1)$.

4 Assorted Problems

Problem #16 Prove that

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$

Problem #17 (Putnam 1973) Given an collection of $2n + 1$ integers such that – if you remove any one of them, the remaining numbers may be divided into two sets of n integers with the same sum. Prove the numbers must all be equal. (Hint: Not inducting on n; actually, first show the numbers must be congruent mod 2)

Problem #18 Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Show that $x^n + \frac{1}{x^n}$ is also an integer for any positive integer n.

Problem #19 The Fermat numbers are defined as follows: $F_n = 2^{2^n} + 1$. Thus, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, etc. Show that the Fermat numbers are pairwise relatively prime (that is, greatest common divisor of any two distinct Fermat numbers is 1).

Induction may be relevant here in relating each Fermat number to the product of all the preceeding Fermat numbers. Note this is another proof of the infinitude of primes.

Problem #20 Prove that in any set of $2^{n+1} - 1$ integers, there is a subset of exactly 2^n of them whose sum is divisible by 2^n.

Problem #21 (USAMO 1978) An integer will be called *good* if it can be written as the sum of positive integers (not necessarily distinct) the sum of whose reciprocals is 1. Given that the integers 33 through 73 are good, prove every integer greater than or equal to 33 is good.

Problem #22 Find all polynomials $P(x)$ that have the property: x is rational if and only if $P(x)$ is rational.

Problem #23 Show that the geometric mean of n positive numbers is always less than or equal to their arithmetic mean. (There are many ways to do this, but one way using induction involves first showing it when $n = 1$, then show how the truth of the result for n yields the truth of it for both $2n$ and $n - 1$. Is this sufficient?)

Problem #24 (1971 Putnam, I think) Given that $q(x) = 3x^2 + 5x + 7$, find all polynomials $p(x)$ (with real coefficients) satisfying $p(0) = 0$ and $p(q(x)) = q(p(x))$ for all real x.

Problem #25 In any graph (with at least two vertices, and disallowing any edges that connect a vertex to itself), at least two vertices have the same number of edges. (in any group of people, at least two have the same number of friends, if friendship is interpreted as a symmetric, non-reflexive relationship).

Problem #26 (Bridges of Königsburg) In a connected graph, if two of the vertices have an odd number of edges and the rest have an even number of edges, it is possible to travel through the graph, using every edge exactly once.

(you can also do this if all the vertices have an even number of edges, and you'll end on the same vertex on which you began.)

Problem #27 For any prime p, and any integer $n \geq p$, show that $\binom{n}{p} \equiv \lfloor n/p \rfloor \bmod p$.

Problem #28 (Dutch-Flemish, 1996?– but older, and well-known) Given a finite collection of of sets, closed under union (that is, if A and B are sets belonging to the collection, then $A \cup B$ is also a set in the collection.) Prove or disprove: there exists an element x that belongs to at least half the sets in the collection.

Hint: if there is any set with only 1 element in it, the proof is immediate.

Problem #29 Show that every integer n may be written as $\pm 1^2 \pm 2^2 \pm 3^2 \ldots \pm k^2$ for some k and some choice of either "+" or "-" for each term.

Problem #30 Prove Euler's Formula (Vertices + Faces - Edges = 2, for either polyhedron or connected planar graphs, suitably interpreted) using induction on number of faces. (The smallest case requires some clarification: it must have at least one vertex, but not necessarily any edges. Also, we need to accept that if there is only one face, the graph must be a tree, i.e. have no cycles.)

Problem #31 Prove Euler's Formula using induction on number of vertices. (contraction)

Problem #32 Prove Euler's Formula using induction on number of edges.

Problem #33 Using Euler's formula, prove that every planar graph must have at least one vertex that has at most five edges. Use this to show that it is possible to color the vertices of any planar graph using 6 colors so that no to vertices joined by an edge are the same color.

Problem #34 Evaluate:

$$\lim_{n\to\infty} \cos\frac{\pi}{2^2} \cdot \cos\frac{\pi}{2^3} \cdots \cos\frac{\pi}{2^n}$$