Math 3012

Lecture 6 - Induction and Euclidean algorithm

Luís Pereira

Georgia Tech

August 31, 2018

The Principle of Mathematical Induction

Well ordering principle/axiom

Any non-empty set of positive integers has a smallest element.

Another formulation

If A is a set of positive integers such that

- 1 is in A
- whenever k is in A then $k + 1$ is also in A

then A is the set of all positive integers.

Consequence: Mathematical Induction

To show that a statement S_n is true for all n, it is enough to check the following two things:

- **Base case:** S_1 is true
- **Induction step:** assuming that S_k is true, show that then S_{k+1} is also true.

Applying Induction (2)

Theorem The sum of the first n odd positive integers is n^2, i.e.

$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2 \qquad (S_n)$$

Proof We apply mathematical induction:

- **Base case** When $n = 1$ the LHS is 1 and RHS is $1^2 = 1$. So S_1 is true.
- **Induction step**. Assume S_k is true, i.e. $1 + 3 + \cdots + (2k - 1) = k^2$. Then

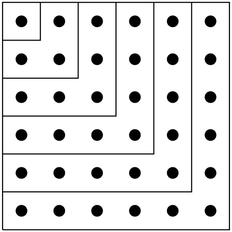
$$\begin{aligned} 1 + 3 + \cdots + (2k - 1) + (2k + 1) &= k^2 + (2k + 1) \quad (\text{by } S_k) \\ &= (k + 1)^2 \end{aligned}$$

  This shows S_{k+1}. QED

Combinatorial proofs versus formal inductive proofs

Recall In Lecture 2 we gave a combinatorial proof of

$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$$



Remarks

- Usually combinatorial proofs are preferable over formal inductive proofs, since they help understand what's really going on. (but "usually" doesn't mean "always")
- Sometimes combinatorial proofs are easier, sometimes inductive proofs are easier (no hard rules).

Applying Induction (3)

Theorem For all positive integer n

$$n^3 + (n+1)^3 + (n+2)^3$$

is a multiple of 9.

Proof We apply mathematical induction:

- **Base case** When $n = 1$ get $1^2 + (1+2)^2 + (1+2)^3 = 36$. This is a multiple of 9 so S_1 is true.
- **Induction step**. Assume S_k is true.

$$\begin{aligned}
&(k+1)^3 + (k+2)^3 + (k+3)^3 = \\
&= (k+1)^3 + (k+2)^3 + k^3 + 9k^2 + 27k + 27 \\
&= \left[k^3 + (k+1)^3 + (k+2)^3\right] + \left[9k^2 + 27k + 27\right]
\end{aligned}$$

Both parts are multiples of 9 (why?), so S_{k+1} is true. QED

Exercises in mathematical induction (1)

Exercise Let $x > -1$ be a real number. Show that for all $n \geq 0$ it is

$$(1+x)^n \geq 1 + nx \qquad (S_n)$$

Solution We apply mathematical induction:

- **Base case** When $n = 0$ the LHS is $(1+x)^0 = 1$ and the RHS is $1 + 0x = 1$. So S_0 is true.
- **Induction step**. Assume S_k is true, i.e.

$$(1+x)^k \geq 1 + kx$$

It follows that (why?)

$$(1+x)^{k+1} \geq (1+kx)(1+x)$$
$$(1+x)^{k+1} \geq 1 + kx + x + kx^2$$
$$(1+x)^{k+1} \geq 1 + (k+1)x + kx^2$$

This implies

$$(1+x)^{k+1} \geq 1 + (k+1)x$$

which is S_{k+1}. QED

Exercises in mathematical induction (2)

Exercise Show that for all integers $n \geq 2$ it is

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$$

Solution

- **Base case** When $n = 2$ we need

$$1 + \frac{1}{\sqrt{2}} > \sqrt{2} \qquad \text{(true?)}$$

This is equivalent to

$$\left(1 + \tfrac{1}{\sqrt{2}}\right)^2 > (\sqrt{2})^2 \quad \text{(true?)}$$

$$1 + \tfrac{2}{\sqrt{2}} + \tfrac{1}{2} > 2 \qquad \text{(true?)}$$

$$\sqrt{2} > 1/2 \qquad \text{(true!)}$$

So S_2 is true.

Exercises in mathematical induction (2.1)

Exercise Show that for all $n \geq 2$ it is

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$$

Solution (cont.)

- **Induction step** Assume S_k, i.e.

  $$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} > \sqrt{k}$$

  Then

  $$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k} + \frac{1}{\sqrt{k+1}}$$

  but what we want to show is

  $$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1}$$

  So it's enough to show $\sqrt{k} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1}$

Exercises in mathematical induction (2.2)

Solution (cont.) It's enough to show

$$\sqrt{k} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1} \qquad \text{(true?)}$$

This is equivalent to

$$\left(\sqrt{k} + \tfrac{1}{\sqrt{k+1}}\right)^2 > \left(\sqrt{k+1}\right)^2 \quad \text{(true?)}$$

$$k + \tfrac{2\sqrt{k}}{\sqrt{k+1}} + \tfrac{1}{k+1} > k+1 \qquad \text{(true?)}$$

$$\tfrac{2\sqrt{k}}{\sqrt{k+1}} + \tfrac{1}{k+1} > 1 \qquad \text{(true?)}$$

This will be true if

$$\tfrac{2\sqrt{k}}{\sqrt{k+1}} > 1 \qquad \text{(true?)}$$

$$2\sqrt{k} > \sqrt{k+1} \quad \text{(true?)}$$

$$4k > k+1 \qquad \text{(true!)}$$

So the top inequality is true. QED (Phew!)

Exercises in mathematical induction (3)

Exercise Show that for every $n \geq 5$ it is

$$n^2 > 3n + 9 \qquad (S_n)$$

Solution We apply mathematical induction:

- **Base case** When $n = 5$ the LHS is $5^2 = 25$ and the RHS is $3 \times 5 + 9 = 24$. Since $25 > 24$ we have S_5 is true.
- **Induction step**. Assume S_k is true, i.e.

  $$k^2 > 3k + 9$$

  Then

  $$(k+1)^2 = k^2 + 2k + 1 > 3k + 9 + 2k + 1 = 3(k+1) + (2k+7)$$

  But we want

  $$(k+1)^2 > 3(k+1) + 9$$

  So we need $2k + 7 \geq 9$. Is this true? Yes! QED

Piazza poll

Question Let S_n be the statement

$$n^2 + n \text{ is a multiple of } 5 \qquad (S_n)$$

Then

Answers

(A) S_4 and S_9 are both true

(B) S_4 is true but S_9 is false

(C) S_4 is false but S_9 is true

(D) S_4 and S_9 are both false

Alternative forms of Mathematical Induction

By contradiction Assume that there is a smallest n such that S_n fails, then argue that S_k must also have failed for some $k < n$, leading to a contradiction.

Strong induction To show that a statement S_n is true for all n, it is enough to check the following two things:

- **Base case:** S_1 is true
- **Strong Induction step:** assuming that all of $S_1, S_2, S_3, \cdots, S_k$ are true, show that then S_{k+1} is also true.

Exercise in strong mathematical induction

Exercise Show that the sequence with recursive definition

$$r_1 = 1; r_2 = 3; , \qquad r_n = r_{n-1} + 2r_{n-2} + 2 \quad \text{for } n \geq 3$$

is given by $r_n = 2^n - 1$.

Solution We apply strong mathematical induction:

- **Base case** $r_1 = 1$ and $2^1 - 1 = 1$ so S_1 holds.
- **Strong induction step** Assume $S_1, S_2, \cdots, S_k$, i.e. that $r_i = 2^i - 1$ when $i \leq k$. Then

  $$r_{k+1} = r_k + 2r_{k-1} + 2 = (2^k - 1) + 2(2^{k-1} - 1) + 2 = 2 \cdot 2^k - 1 = 2^{k+1} - 1$$

  This shows S_{k+1} when $k + 1 \geq 3$.

  Must still check S_2 explicitly!!
  But $r_2 = 3 = 2^3 - 1$ so we're good. QED

Greatest common divisors (1)

Elementary problem: Adding fractions

$$\frac{5}{12} + \frac{7}{30} = \frac{5 \cdot 5}{12 \cdot 5} + \frac{7 \cdot 2}{30 \cdot 2} = \frac{39}{60} = \frac{13}{20}$$

Upshot Adding fractions is all about least common multiples and greatest common divisors.

Remark Given positive integers n, m

$$gcd(n, m) \cdot lcm(n, m) = n \cdot m$$

Upshot Finding *gcd* and *lcm* are problems of the same difficulty.

Greatest common divisors (2)

Less elementary problem: Adding big fractions

$$\frac{7871827128979}{98823030133990122859735822} + \frac{1273872987897293}{8228883759908824 7} = ?$$

Basic issue Finding

$$gcd(98823030133990122859735822, 82288837599088247)$$

Solutions (?)

- Test all numbers up to 82288837599088247, pick the biggest number that divides both numbers
- Find the prime factorizations of both numbers, take common prime factors

These technically work, but are very inefficient.
A better way is given by the *Euclidean Algorithm*.

Basis for long division & the Euclidean Algorithm (1)

Theorem Let n, m be positive integers. Then there are unique q and r with $q \geq 0$ and $m > r \geq 0$ such that

$$n = qm + r$$

Set-up Fix $m \geq 2$ and let S_n be "there exist $q \geq, n > r \geq 0$ with $n = qm + r$"

Proof By induction on n

- **Base Case** $1 = 0 \times m + 1$, so S_1 is true.
- **Induction Step** Assume S_k, i.e. $k = qm + r$. Two cases:
  - $r < m - 1$ Then $k + 1 = qm + (r + 1)$ works.
  - $r = m - 1$ Then $k + 1 = qm + m - 1 + 1 = (q + 1)m + 0$ works

  In either case we get S_{k+1}.
  The uniqueness part follows from basic algebra. QED

Basis for long division & the Euclidean Algorithm (2)

Theorem Let n, m be positive integers. Then there are unique q and r with $q \geq 0$ and $m > r \geq 0$ such that

$$n = qm + r$$

Fact If $r = 0$ then $gcd(n, m) = m$

Fact If $r > 0$ then $gcd(n, m) = gcd(m, r)$

Why? $\frac{n}{d} = q\frac{m}{d} + \frac{r}{d}$ and $\frac{r}{d} = \frac{n}{d} - q\frac{m}{d}$

Notation $r = n\%m$

The Euclidean Algorithm

Euclidean Algorithm

```
def gcd(n,m):
    if n % m == 0:
        return m
    else:
        return gcd(m,n%m)
```

Idea Perform long division with smaller and smaller numbers until it stops.

The Euclidean Algorithm in action

Question Find $gcd(10262736, 85470)$.

Answer

$$\begin{array}{rcrcr} 10262736 & \% & 85470 & = & 6336 \\ 85470 & \% & 6336 & = & 3102 \\ 6336 & \% & 3102 & = & 132 \\ 3102 & \% & 132 & = & 66 \\ 132 & \% & 66 & = & 0 \end{array}$$

Hence $gdc = 66$.