CS 70: Discrete Math and Probability

Happy Monday!

Today:
Finish Note 2.
Begin Induction.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider number

$$q = (p_1 \times p_2 \times \cdots p_k) + 1.$$

- q cannot be one of the primes as it is larger than any p_i.
- q has prime divisor p ("$p > 1$" = R) which is one of p_i.
- p divides both $x = p_1 \cdot p_2 \cdots p_k$ and q, and divides $q - x$,
- $\implies p | q - x \implies p \leq x - q = 1$. That is, $p|1$.
- so $p \leq 1$. (**Contradicts** R.)

The original assumption that "the theorem is false" is false, thus the theorem is proven. $\square$

Product of first k primes..

Did we prove?

- "The product of the first k primes plus 1 is prime."
- No.
- The chain of reasoning started with a false statement.

Consider example..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 30031$ that divides q.
- Proof assumed no primes *in between* p_k and q.

Proof by cases.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.
Proof: First a lemma...

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, *then both a and b are even.*

Reduced form $\frac{a}{b}$: a and b can't both be even! + Lemma
$\implies$ no rational solution. $\square$

Proof of lemma: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - \frac{a}{b} + 1 = 0$$

Multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even. Not possible.
Case 2: a even, b odd: even - even +odd = even. Not possible.
Case 3: a odd, b even: odd - even +even = even. Not possible.
Case 4: a even, b even: even - even +even = even. Possible.

The fourth case is the only one possible, so the lemma follows. $\square$

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
- $$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^2 = 2.$$

Thus, we have irrational x and y with a rational x^y (i.e., 2).

One of the cases is true so theorem holds. $\square$

Question: Which case holds? Don't know!!!

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$.

Start with $12 = 12$.

Divide one side by 3 and the other by 4 to get
$4 = 3$.

By commutativity theorem holds. $\square$

Don't assume what you want to prove!

Be really careful!

Theorem: $1 = 2$
Proof: For $x = y$, we have

$$(x^2 - xy) = x^2 - y^2$$
$$x(x-y) = (x+y)(x-y)$$
$$x = (x+y)$$
$$x = 2x$$
$$1 = 2 \qquad \square$$

Dividing by zero is no good.

Also: Multiplying inequalities by a negative.

$P \implies Q$ does not mean $Q \implies P$.

Summary: Note 2.

Direct Proof:
To Prove: $P \implies Q$. Assume P. Prove Q.

By Contraposition:
To Prove: $P \implies Q$ Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
To Prove: P Assume $\neg P$. Prove False .

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
or $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$ worked.

Careful when proving!
Don't assume the theorem. Divide by zero.Watch converse. ...

Note 3.

Principle of Induction.

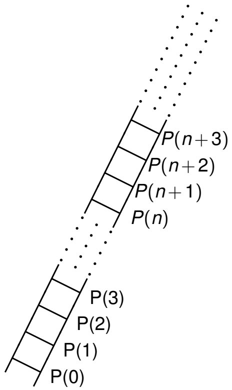
$$P(0) \wedge (\forall n \in \mathbb{N}) P(n) \implies P(n+1)$$

And we get...

$$(\forall n \in \mathbb{N}) P(n).$$

...Yes for 0, and we can conclude Yes for 1...
and we can conclude Yes for 2.......

Climb an infinite ladder?



$$P(0)$$
$$\forall k, P(k) \implies P(k+1)$$
$$P(0) \implies P(1) \implies P(2) \implies P(3) \ldots$$
$$(\forall n \in N) P(n)$$

Your favorite example of forever..or the natural numbers...

Another Induction Proof.

Theorem: For every $n \in N$, $n^3 - n$ is divisible by 3. $(3|(n^3 - n)$).

Proof: By induction.
Base Case: $P(0)$ is "$(0^3) - 0$" is divisible by 3. Yes!
Induction Step: $(\forall k \in N), P(k) \implies P(k+1)$
Induction Hypothesis: $k^3 - k$ is divisible by 3.
or $k^3 - k = 3q$ for some integer q.

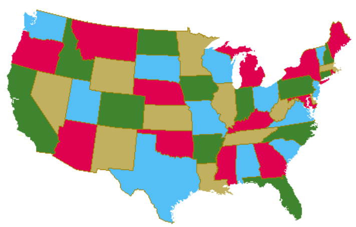
$$\begin{aligned}(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - (k+1)\\ &= k^3 + 3k^2 + 2k\\ &= (k^3 - k) + 3k^2 + 3k && \text{Subtract/add } k\\ &= 3q + 3(k^2 + k) && \text{Induction Hyp.} \quad \text{Factor.}\\ &= 3(q + k^2 + k) && \text{(Un)Distributive} + \text{over} \times\end{aligned}$$

Or $(k+1)^3 - (k+1) = 3(q + k^2 + k)$.

$(q + k^2 + k)$ is integer (closed under addition and multiplication).
$\implies (k+1)^3 - (k+1)$ is divisible by 3.
Thus, $(\forall k \in N) P(k) \implies P(k+1)$
Thus, theorem holds by induction. $\square$

Four Color Theorem.

Theorem: Any map can be colored so that those regions that share an edge have different colors.

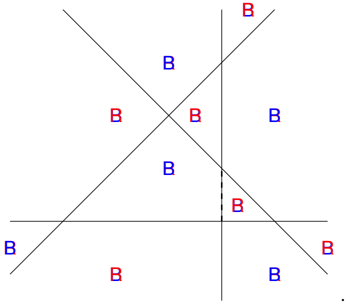


Check Out: "Four corners".
States connected at a point, can have same color.
(Couldn't find a map where they did though.)

Quick Test: Which states? Utah. Colorado. New Mexico. Arizona.

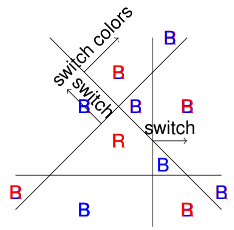
Two color theorem: example.

Any map formed by dividing the plane into regions by drawing straight lines can be properly colored with two colors.



Fact: Swapping red and blue gives another valid colors.

Two color theorem: proof illustration.



Base Case.
1. Add line.
2. Get inherited color for split regions
3. Switch on one side of new line.

(Fixes conflicts along line, and makes no new ones.)

Algorithm gives $P(k) \implies P(k+1)$. □

Review Argument: $P(k) \implies P(k+1)$.

Add line.
Inherit Colors.
Switch colors on one side of line.

For any "edge".
 Ok before switch. Still ok, by "fact".
 Not ok before switch, must be on new line.
  Switch changes one side,
   So now two sides have different colors.

Wrapup.

Proofs: Direct, By Contraposition, By Cases, By Contradiction.

Induction:
 First Step (Base case).
 Can step up the ladder of naturals. (Induction Step.)
Get to be on step k. (Use induction hypothesis.)

See you on Wednesday!