Basic Proof Methods

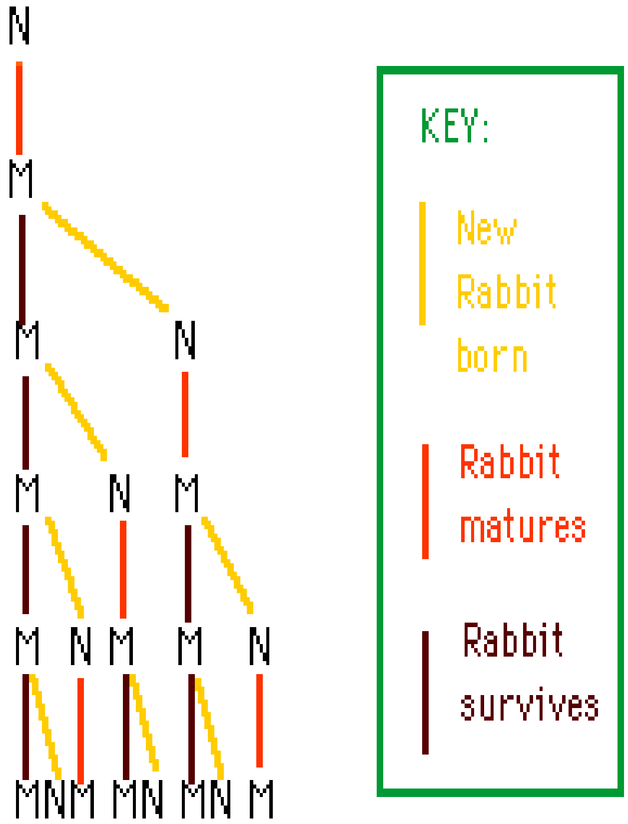
HWW Math Club Meeting #3 (October 18, 2010)

Presentation by Julian Salazar

INTRO: RABBITS!

- You start with one pair of young rabbits (N)
- After one month, all pairs of young rabbits mature (M)
- Every month afterwards, each mature pair survives and produces one pair of young rabbits
- Is there a pattern to the number of rabbit pairs?

Intro: RABBITS!



Fun fact: In 37 months, there would be more rabbits than Canadians

Direct Proof

- Establishing a new fact directly from previously known facts without making any assumptions

Divisibility

$6 \mid 360$

$1 \mid 43$

$11 \mid 121$

$11 \mid 11$

$11 \nmid 111$

$12 \nmid 23$

Primes have exactly two distinct factors; itself and 1.

Two numbers are coprime when gcd(a,b) = 1.

All numbers divide 0.

Divisibility and Direct Proof

- Find, with proof, all integers $n \geq 1$ such that $n^3 - 1$ is prime.

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

For $n^3 - 1$ to be prime, exactly one of $(n^2 + n + 1)$ and $(n - 1)$ must equal 1.

$$n^2 + n + 1 \neq 1 \ \forall\ n \in \mathbb{Z}^+$$

$$n - 1 = 1 \text{ iff } n = 2 \ \forall\ n \in \mathbb{Z}^+$$

$$n^3 - 1 \ \forall\ n \in \mathbb{Z}^+ \text{ is prime iff } n = 2 \ ▪$$

Modular (Clock) Arithmetic

$81 \equiv 0 \pmod{9}$

$56 \equiv 0 \pmod{7}$

$7 \equiv 3 \pmod{4}$

$899 \equiv -1 \pmod{9}$

$15 \equiv 9 \pmod{6} \equiv 3 \pmod{6}$

$31458734123124^{102} \equiv 1 \pmod{103}$

Addition, multiplication, and subtraction always work on both sides of the congruence.

…BUT NOT DIVISION D=<

(well, not regular division)

Modular Arithmetic

Prove that 314159265358 cannot be written as the sum of any number of even square numbers.

$$n_1^2 + n_2^2 + \ldots + n_i^2 \neq 314159265358 \ \forall \{n_i \mid 2 \mid n_i, i \in \mathbb{Z}^+\}$$

Note that $n^2 \equiv 0 \pmod 4$ $\forall$ even numbers.

Note that $314159265358 \equiv 2 \pmod 4$.

$$0 \pmod 4 + 0 \pmod 4 + \ldots \neq 2 \pmod 4. \ \blacksquare$$

Proof by Contradiction

If you have a statement you want to prove:

Assume the logical negative.

IF

You reach a contradiction

THEN

The original statement must be true.

Proof by Contradiction

Prove $(21n + 4) / (14n + 3)$ is in lowest terms for all non-zero integers n. (IMO, 1959)

Proof: Contradiction.

Assume the fraction is not in lowest terms.

There exists $|x| > 1$ such that $x \mid 21n + 4$ and $x \mid 14n + 3$.

$$21n + 4 \equiv 0 \bmod x \rightarrow 42n + 8 \equiv 0 \bmod x$$

$$14n + 3 \equiv 0 \bmod x \rightarrow 42n + 9 \equiv 0 \bmod x$$

This is impossible for integers $|x| > 1$, so our assumption must be false and the original statement is true. ▪

Proof by Induction

If a statement is true for a base case

AND

If being true for one case makes it true for the next case

THEN

It is true for all cases.

Proof by Induction

Prove that you can knock over dominoes arranged standing beside each other.

a.) Base Case: You can knock over the first domino.

b.) Inductive Hypothesis: When any domino is knocked over, the one after it is also knocked over.

Therefore, all the dominoes will be knocked over.

Proof by Induction

Theorem: $7^n - 1$ is divisible by 6 for all whole numbers n.

Proof: Induction

i.) Base case: $7^0 - 1 = 0$, and $6 \mid 0$

ii.) Inductive hypothesis: Suppose $6 \mid 7^n - 1$.

$$7^{n+1} - 1 = 7(7^n) - 1$$
$$= 6(7^n) + 7^n - 1.$$

By induction, the theorem is true. ▪

TEH ENDS

Did you know that…

the area of all simple lattice polygons P are expressible in terms of the number of lattice points on its boundary and its interior? (Pick's Theorem)

Did you know that…

there is a closed-form formula that generates the nth term of the Fibonacci sequence:

$$F(n) = \frac{\varphi^n - (1-\varphi)^n}{\sqrt{5}} = \frac{\varphi^n - (-1/\varphi)^n}{\sqrt{5}},$$

Can you prove why it works?