START RECORDING

Disprove by Counterexample and Prove by Example

Disprove by Counterexample

Conjecture

- Conjecture
  - Let $tens(n)$ be the tens digit of n
  - Let $ones(n)$ be the ones digit of n
  - Let $diff(n) = |tens(n) - ones(n)|$
  - Bill thinks that $(\forall\ n \in \mathbb{N})[DIFF(n^2) \leq 6]$

Conjecture

- Conjecture
  - Let $tens(n)$ be the tens digit of n
  - Let $ones(n)$ be the ones digit of n
  - Let $diff(n) = |tens(n) - ones(n)|$
  - Bill thinks that $(\forall\, n \in \mathbb{N})[DIFF\left(n^2\right) \leq 6]$
- To PROVE this we would need to prove it for EVERY n

Conjecture

- Conjecture
  - Let $tens(n)$ be the tens digit of n
  - Let $ones(n)$ be the ones digit of n
  - Let $diff(n) = |tens(n) - ones(n)|$
  - Bill thinks that $(\forall\, n \in \mathbb{N})[DIFF\left(n^2\right) \leq 6]$
- To PROVE this we would need to prove it for EVERY n
- To DISPROVE it we only need to find ONE n for which it is false.

Data for n = 4, 5, 6, 7, 8, 9

n	n^2	$DIFF(n^2)$
4	16	5
5	25	3
6	36	3
7	49	5
8	64	2
9	81	7

Data for n = 4, 5, 6, 7, 8, 9

n	n^2	$DIFF(n^2)$
4	16	5
5	25	3
6	36	3
7	49	5
8	64	2
9	81	7

- Keep doing this until get to counterexample.

Data for n = 4, 5, 6, 7, 8, 9

n	n^2	$DIFF(n^2)$
4	16	5
5	25	3
6	36	3
7	49	5
8	64	2
9	81	7

- Keep doing this until get to counterexample.
- Then conjecture will be
  - We have disproven the conjecture since for 9^2 the diff is 7.

Now What?

- The following questions remain
  1) Maybe the conjecture is true past some point. Maybe
  $$(\exists\, n_0)(\forall\, n \geq\ n_0)[\text{diff}(n^2) \leq\ 6]$$
  2) Maybe 6 is to low. So maybe
  $$(\forall\, n \geq\ 4)[\text{diff}(n^2) \leq\ 7]$$
  3) Maybe item 2 is incorrect but holds past some point, so
  $$(\exists\, n_0)(\forall\, n \geq\ n_0)[\ \text{diff}(n^2) \leq\ 7]$$

Prove By Example

- We just showed that
  - You can DISPROVE $(\forall\, x)[P(x)]$ by showing just ONE x for which $\neg\, P(x)$ is TRUE.

Prove By Example

- We just showed that
  - You can DISPROVE $(\forall\ x)[P(x)]$ by showing just ONE x for which $\neg\ P(x)$ is TRUE.
- Same Idea but stated differently:
  - You can PROVE $(\exists\ x)[P(x)]$ by showing just ONE x for which $P(x)$ is TRUE.

Prove By Example

- We just showed that
  - You can DISPROVE $(\forall\ x)[P(x)]$ by showing just ONE x for which $\neg\ P(x)$ is TRUE.
- Same Idea but stated differently:
  - You can PROVE $(\exists\ x)[P(x)]$ by showing just ONE x for which $P(x)$ is TRUE.
- In either case we need to show that some x with some property exists.

Constructive proofs in Number Theory
(and one non-constructive one)

Our first constructive proof

- **Claim** There exists a natural number that you ***cannot*** write as a sum of three squares of natural numbers.
  - Examples of numbers you ***can*** write as a sum of three squares
    - $0 = 0^2 + 0^2 + 0^2$
    - $1 = 1^2 + 0^2 + 0^2$
    - $2 = 1^2 + 1^2 + 0^2$
- Try to find a number that ***cannot*** be written as such.

Proof

- The natural number 7 cannot be written as the sum of three squares.
- This we can prove by case analysis
  1. Can't use 3, since $3^2 = 9 > 7$
  2. Can't use 2 more than once, since $2^2 + 2^2 = 8 > 7$
  3. So, we can use 2, one or zero times.
     a) If we use 2 once, we have $7 = 2^2 + a^2 + b^2 \leq 2^2 + 1^2 + 1^2 = 6 < 7$
     b) If we use 2 zero times, the maximum value is $1^2 + 1^2 + 1^2 = 3 < 7$
  4. Done!

Let’s Go Further!

- We showed that there exists x (namely 7) so that x cannot be written as the sum of 3 squares.
  - This is the origin of 7 being a lucky number.

Let’s Go Further!

- We showed that there exists x (namely 7) so that x cannot be written as the sum of 3 squares.
  - This is the origin of 7 being a lucky number.
- That last sentence is not true. Emily no longer believes anything I say since
  - I lied in Ramsey Theory every other day.
  - (More like 4 times a day…)

Let’s Go Further!

- We showed that there exists x (namely 7) so that x cannot be written as the sum of 3 squares.
  - This is the origin of 7 being a lucky number.
- That last sentence is not true. Emily no longer believes anything I say since
  - I lied in Ramsey Theory every other day.
  - (More like 4 times a day…)
- But seriously, are there more numbers that cannot be written as the sum of three squares?
  - This is not our original question, but its a good question, so we pursue it.

Sum of Three Squares

- In Breakout Rooms, Find
  - Other numbers that are NOT the sum of 3 squares
  - Try to prove there are an INFINITE number of numbers that are NOT the sum of 3 squares

Sum of Three Squares

n	n as a sum of squares	Number of squares ≤ 3
1	1^2	Y
2	$1^2 + 1^2$	Y
3	$1^2 + 1^2 + 1^2$	Y
4	2^2	Y
5	$2^2 + 1^2$	Y
6	$2^2 + 1^2 + 1^2$	Y
7	$2^2 + 1^2 + 1^2 + 1^2$	N
8	$2^2 + 2^2$	Y

Sum of Three Squares

n	n as a sum of squares	Number of squares ≤ 3
9	3^2	Y
10	$3^2 + 1^2$	Y
11	$3^2 + 1^2 + 1^2$	Y
12	$2^2 + 2^2 + 2^2$	Y
13	$3^2 + 2^2$	Y
14	$3^2 + 2^2 + 1^2$	Y
15	$3^2 + 2^2 + 1^2 + 1^2$	N
16	4^2	Y

Sum of Three Squares

n	n as a sum of squares	Number of squares ≤ 3
17	$4^2 + 1^2$	Y
18	$3^2 + 3^2$	Y
19	$3^2 + 3^2 + 1^2$	Y
20	$4^2 + 2^2$	Y
21	$4^2 + 2^2 + 1^2$	Y
22	$3^2 + 3^2 + 2^2$	Y
23	$3^2 + 3^2 + 2^2 + 1^2$	N
24	$4^2 + 2^2 + 2^2$	Y

Sum of Three Squares

- If $n \equiv 7\ (mod\ 8)$, then n CANNOT be written as the sum of 3 squares

Mod 8	
$0^2 \equiv 0$	$4^2 \equiv 0$
$1^2 \equiv 1$	$5^2 \equiv 1$
$2^2 \equiv 4$	$6^2 \equiv 4$
$3^2 \equiv 1$	$7^2 \equiv 1$

Sum of Three Squares

So, is there some way for three numbers from 0, 1, 4 to add up to $7(mod\ 8)$?

Case 1 Use *zero* 4's. Then max is 1+1+1≡3 < 7.

Case 2 Use exactly *one* 4. Then we have to get 3 with two of {0,1}, but the max is 1+1 ≡ 2 < 4.

Case 3 Use *two* 4's 4+4+0=1, 4+4+1 ≡ 2.

Case 4 Use *three* 4's 4+4+4 ≡ 4.

What do we know?

- Theorem: If $n \equiv\ 7 \pmod 8$ then 7 cannot be written as the sum of 3 squares.

What do we know?

- Theorem: If $n \equiv 7 \pmod 8$ then 7 cannot be written as the sum of 3 squares.
- Conjecture: The only numbers that cannot be written as the sum of 3 squares are those that are $\equiv 7 \pmod 8$.

What do we know?

- Theorem: If $n \equiv 7 \pmod 8$ then 7 cannot be written as the sum of 3 squares.
- Conjecture: The only numbers that cannot be written as the sum of 3 squares are those that are $\equiv 7 \pmod 8$.
- Is this true? You may investigate it on a Homework.

Your turn, class!

- Let's break into breakout rooms and prove the following theorems

1. There exists an integer n that can be written in ***two ways*** as a sum of two prime numbers.
2. There is a **perfect square** that can be written as a sum of two other **perfect squares**.
3. Suppose $r, s \in \mathbb{Z}$. Then, $(\exists k \in \mathbb{Z})[\, 22r + 18s = 2k]$

Our first non-constructive proof

- Theorem There exists a pair of irrational numbers a and b such that a^b is a rational number.

Our first non-constructive proof

- For the following proof, we will assume *known* that $\sqrt{2} \notin \mathbb{Q}$.
- This is a *fact*, which we will prove later on in this section.
- Now, on to the proof!

Our first non-constructive proof

- **Theorem** There exists a pair of irrational numbers a and b such that a^b is a rational number.

Our first non-constructive proof

- **Theorem** There exists a pair of irrational numbers a and b such that a^b is a rational number.
- **Proof** Let $a = b = \sqrt{2}$. Since $\sqrt{2}$ is irrational, a and b are both irrational. Is $a^b = (\sqrt{2})^{\sqrt{2}}$ **rational**? Two cases

Our first non-constructive proof

- **Theorem** There exists a pair of irrational numbers a and b such that a^b is a rational number.
- **Proof** Let $a = b = \sqrt{2}$. Since $\sqrt{2}$ is irrational, a and b are both irrational. Is $a^b = (\sqrt{2})^{\sqrt{2}}$ **rational**? Two cases
  1. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have proven the result. Done.

Our first non-constructive proof

- **Theorem** There exists a pair of irrational numbers a and b such that a^b is a rational number.
- **Proof** Let $a = b = \sqrt{2}$. Since $\sqrt{2}$ is irrational, a and b are both irrational. Is $a^b = (\sqrt{2})^{\sqrt{2}}$ **rational**? Two cases
  1. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have proven the result. Done.
  2. If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we will name it c. Then, observe that $c^{\sqrt{2}}$ is rational, since $c^{\sqrt{2}} = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2 \in \mathbb{Q}$. Since both c and $\sqrt{2}$ are irrationals, but $c^{\sqrt{2}}$ is rational, we are done.

Analysis of proof

- Suppose $x = \sqrt{2}$, an irrational. From the previous theorem, we know
  a) Either that $a = x, b = x$ are two irrationals that satisfy the condition , OR
  b) That $a = x^x, b = x$ are the two irrationals.

- But we **don't care which pair it is**! As long as one exists!

STOP RECORDING