1.8 Proof Methods and Strategy

Exhaustive Proofs

Some Theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs.

Example:

Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer $n \leq 4$.

(note: $\frac{n^3}{3^n} \to 0$ as $n \to \infty$ so we know this shouldn't hold for all $n \geq 0$).

We only need to show this holds for $n = 1, 2, 3$ and 4 so we can prove this by checking each case.

$n=1$: $2^3 = 8 \geq 3 = 3^1$ $\quad$ $n=3$: $4^3 = 64 \geq 27 = 3^3$

$n=2$: $3^3 = 27 \geq 9 = 3^2$ $\quad$ $n=4$: $5^3 = 125 \geq 81 = 3^4$.

Since this is true for all 4 cases we have shown that if n is a positive integer ≤ 4 then $(n+1)^3 \geq 3^n$.

Definition:

An integer n is a perfect power if $n = m^a$ for some integer m and an integer $a > 1$.

Example:

Prove that 8 and 9 are the only consecutive positive perfect powers not exceeding 100.

All we have to do is find all perfect powers not exceeding 100 and see if there are consecutive perfect powers.

Squares: 1, 4, 9, 16, 25, 36, 49, 64, 81, 100

Cubes: 1, 8, 27, 64 6th: 1, 64

4th powers: 1, 16, 81 7th: 1

5th powers: 1, 32,

So the perfect powers are

1, 4, $\underbrace{8, 9}$, 16, 25, 27, 32, 36, 49, 64, 81, 100

Only consecutive ones.

We can only do exhaustitive proofs when there are a finite number of cases to check. (Typically we use computers to check a lot of cases. Like the 4-color theorem.)

Proof by Cases:

Sometimes we can break a theorem into a few cases and prove each case. It is important to make sure the cases cover everything possible.

Example:

Prove that if n is an integer, then $n^2 \geq n$.

Three case: ① $n>0$ ② $n<0$ ③ $n=0$.

① If $n>0$ then $n \geq 1$. So,

$n^2 \geq n \cdot 1 = n$. Hence, $n^2 \geq n$.

② If $n<0$ then $n \leq -1$. so,

$n^2 \geq 0 > n$. Hence, $n^2 \geq n$.

③ If $n=0$ then $n^2 = 0 = n$. Hence, $n^2 \geq n$.

Example:

Use proof by cases to show that

$|xy| = |x||y|$.

We have 4 cases:

① $x \geq 0, y \geq 0$ ② $x \geq 0, y<0$ ③ $x \geq 0, y \geq 0$

④ $x<0, y<0$.

① Since $x \geq 0$ and $y \geq 0$ we know that $xy \geq 0$.
Furthermore by definition of abs. value
$|xy| = xy$ and $|x| = x$, $|y| = y$. Therefore

$$|xy| = xy = x \cdot y = |x| \cdot |y|.$$

② Since $x \geq 0$ and $y < 0$ we know that $xy \leq 0$.
Furthermore by definition of abs. value
$|xy| = -xy$ and $|x| = x$, $|y| = -y$. Therefore

$$|xy| = -xy = x \cdot (-y) = |x| \cdot |y|.$$

③ Switch x and y in the argument for ②.

④ Since $x < 0$ and $y < 0$ we know that $xy > 0$.
Furthermore by definition of abs. value
$|xy| = xy$ and $|x| = -x$, $|y| = -y$. Therefore,

$$|xy| = xy = (-x)(-y) = |x||y|. \blacksquare$$

Remark: Generally look for a proof by cases when there is no obvious way to begin a proof, but when extra information in each case helps move the argument forward.

Example:

Formulate a conjecture about the final digit of the square of an integer and prove the conjecture.

What are the final digits?

1 2 3 4 5 6 7 8 9 10 11 12

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144

1 4 9 6 5 6 9 4 1 0 1 4

looks like it starts repeating and

only 1, 4, 9, 6, 5, 0 show up.

<u>Conjecture</u>: Last digit is 0, 1, 4, 5, 6 or 9.

Last digit seems to be determined by the last digit of what we are squaring. What this means is that if we write the number as $10a+b$ where a is an integer and b is an integer such that $0 \le b \le 9$, then the last digit of $(10a+b)^2$ is determined by b. Note that

$$(10a+b)^2 = \underbrace{100a^2+10ab}_{\text{does not contribute to the last digit.}} + b^2 = 10(10a^2+ab)+b^2.$$

Additionally, $(10-b)^2 = 100-20b+b^2 = 10(10-2b)+b^2$

This implies that b^2 and $(10-b)^2$ have the same last digit. So we have the following cases to check

1. $b=0$
2. $b=1$ $10-b=9$
3. $b=2$ $10-b=8$
4. $b=3$ $10-b=7$
5. $b=4$ $10-b=6$
6. $b=5$

1. $0^2=0$
2. $1^2=1$ so 9^2 has the last digit 1.
3. $2^2=4$
4. $3^2=9$
5. $4^2=16$ which has the last digit 6.
6. $5^2=25$ which has the last digit 5

Combining the cases we can conclude that $\forall n \in \mathbb{Z}$ the final digit of n^2

is $0, 1, 2, 4, 5, 6$ or 9.

Example:

Show that there are no solutions in integers x and y of $x^2+3y^2=8$.

Note: If $x^2>8$ or $3y^2>8$ then this cannot be a solution since then $x^2+3y^2>8$, because $x^2, 3y^2 \geq 0$.

So we can reduce this to checking $x^2 \leq 8$ and $3y^2 \leq 8$. So, $x = 0, 1, 2, -1,$ or -2 and $y = 0, 1, -1$. Furthermore, all negative values give the same value as the positive so we just need to check $x=0,1,2$ and $y=0,1$.

$x=0, y=0$: $0^2+3(0)^2=0 \neq 8$

$x=0, y=1$: $0^2+3(1^2)=3 \neq 8$

$x=1,\ y=0 \qquad 1^2+3(0)^2=1\neq 8$

$x=1,\ y=1 \qquad 1^2+3(1)^2=4\neq 8$

$x=2,\ y=0 \qquad 2^2+3(0)^2=4\neq 8$

$x=2,\ y=1 \qquad 2^2+3(1)^2=7\neq 8$

Therefore $x^2+3y^2=8$ has no integer solutions.

(Remark: $x^2+3y^2=8$ is an ellipse with an infinite number of real solutions).

Example:

Show that if $x,y\in\mathbb{Z}$ and xy and $x+y$ are even then x and y are even.

Proof by contraposition: Want to show if x or y is odd then xy or $x+y$ is odd. Without loss of generality assume x is odd. We can do this because x is a variable so showing the case where y is odd can be done by just swapping x and y. Since x is odd, $x=2k+1$ for some integer k. Now we have two case ① y is odd ② y is even).

① Suppose y is odd. Then $y=2m+1$ for some integer m. Hence

$$xy=(2k+1)(2m+1)=4mk+2k+2m+1$$
$$=2(2mk+k+m)+1$$

where $2mk+k+m \in \mathbb{Z}$. Therefore, xy is odd.

② Suppose y is even. Then, $y=2m$ for some integer m. Hence,

$$x+y=2k+1+2m=2(m+k)+1 \text{ where}$$
$(m+k) \in \mathbb{Z}$. Hence $x+y$ is odd.

Remark: With exhaustive proofs you need to show every case possible. You cannot use a exhaustive proof for $\forall x (P(x) \to Q(x))$ If the number of elements x such that $P(x)$ is true is infinite.

Example:

Every positive integer is the sum of 18 fourth power integers. This is true up to 78 but is not true for 79

Also, proves by cases must include every possible case. (Don't forget about 0).

Example:

$\forall x \in \mathbb{R} \, (x^2 > 0)$. This is true for the cases ① $x > 0$ and ② $x < 0$ but we can't forget about $x = 0$ where this does not hold.

Existence Proofs

A proof of a proposition of the form $\exists x P(x)$ is an existence proof. Finding an element, a, such that $P(a)$ is a constructive proof. It is possible to show $\exists x P(x)$ in a non constructive way. Typically this is done by assuming $\neg(\exists x P(x))$ and showing this causes a contradiction.

Example:

Show that there exists a positive integer that can be written as the sum of cubes of positive integers in two ways.

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

We just need 1 example.

Example: (Non-constructive Proof)

Show that there exists irrational numbers x and y such that x^y is rational.

Recall that $\sqrt{2}$ is irrational.

Take $x=\sqrt{2}$, $y=\sqrt{2}$. Then either $\sqrt{2}^{\sqrt{2}}$ is rational (in which case we are done) or $\sqrt{2}^{\sqrt{2}}$ is irrational. If $\sqrt{2}^{\sqrt{2}}$ is irrational then $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2$ which is rational.

Hence, either $\sqrt{2}^{\sqrt{2}}$ is rational or $\sqrt{2}^{\sqrt{2}}$ is irrational and $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$ is rational. So either the pair $x=\sqrt{2}$ $y=\sqrt{2}$ or $x=\sqrt{2}^{\sqrt{2}}$ $y=\sqrt{2}$ provides an example

Unique Proofs:

We need to show the existence of an element and then uniqueness

Recall:

$$\exists! x\ P(x) \equiv \exists x (P(x) \wedge \forall y (y \neq x \to \neg P(y)))$$

Typically we show uniqueness by assuming both x and y satisfy $P(x), P(y)$ and then showing $x = y$.

Example:

Show that if a and b are real numbers and $a \neq 0$ then there exists a unique real number r such that $ar + b = 0$.

Give a, b choose $r = -\frac{b}{a}$ which exists since $a \neq 0$. So $ar + b = a(-\frac{b}{a}) + b = -b + b = 0$.

Hence can r exists.

Suppose r_1 and r_2 are such that $ar_1+b=0$ and $ar_2+b=0$. Then $ar_1+b=ar_2+b$. So,

$ar_1=ar_2$. Since $a\neq 0$, $r_1=r_2$. ∎

Sometimes we will want to use backwards reasoning to find the way to prove a statement.

Example:

Show that if $x,y>0$ and $x\neq y$ then

$$\frac{x+y}{2} \geq \sqrt{xy}.$$

Work backwards to something we can show using $x,y>0$ and $x\neq y$.

$$\frac{x+y}{2} > \sqrt{xy}$$

$$\iff \frac{(x+y)^2}{4} > xy, \quad \text{since } x,y > 0.$$

$$\iff (x+y)^2 > 4xy$$

$$\iff x^2+2xy+y^2 > 4xy$$

$$\iff x^2-2xy+y^2 > 0$$

$$\iff (x-y)^2 > 0.$$

Now we want to construct this in the right order.

Suppose $x,y>0$ and $x \neq y$. Then $(x-y)^2>0$. So, $x^2-2xy+y^2>0$. Hence, $x^2+2xy+y^2>4xy$. Thus, $(x+y)^2>4xy$ and $\frac{(x+y)^2}{4}>xy$. Therefore $\frac{x+y}{2}>\sqrt{xy}$.

The idea was we found $p: (x-y)^2 > 0$

such that $p \to q$ was true $q: \frac{x+y}{2} > \sqrt{xy}$.

Then showed $r: (x, y \neq 0, x \neq y)$ $r \to p$

was true. Hence $r \to q$.

Adapting Existing Proofs

We can look at reusing similar strategies.

Example:

Prove that $\sqrt{3}$ is irrational

$\sqrt{3}$

Suppose $\cancel{\sqrt{2}}$ is rational. Then,

$\sqrt{3}$ $\cancel{\sqrt{2}} = \frac{a}{b}$ for some $a,b \in \mathbb{Z}$ and $b \neq 0$.
and such that a,b have no common factors.

Then $\cancel{2}\,3 = \frac{a^2}{b^2}$ or equivalently $\cancel{2}\,3b^2 = a^2$.

Since $b^2 \in \mathbb{Z}$ we know that a^2 is ~~even~~ multiple of 3

Hence a is ~~even~~ multiple of 3, by ~~exercise 10~~ since a is an integer and 3 is prime.

(similar to example n^2 odd $\Rightarrow$ n odd)

So, $a = \cancel{2}\,3c$ for some $c \in \mathbb{Z}$. Then,

$a^2 = \cancel{4}\,9c^2$. From this we can conclude

that $\cancel{2}\,3b^2 = \cancel{4}\,9c^2$ or equivalently

$b^2 = \cancel{2}\,3c^2$. Hence b^2 is ~~even~~ a multiple of 3 and

b must be ~~even~~ a multiple of 3. Hence a,b are both ~~even~~ multiples of 3 and must have a common factor. This contradicts the fact that a,b have no common factors.

We can extend this to $\sqrt{n}$ for any positive n that is not a perfect square.

Looking for Counterexamples

Looking for counterexamples is an important in forming conjectures in math. We typically have some idea of a statement and then look for counterexamples. If we cannot find a counterexample, then we try to prove the conjecture

Example: Fermat's last Theorem

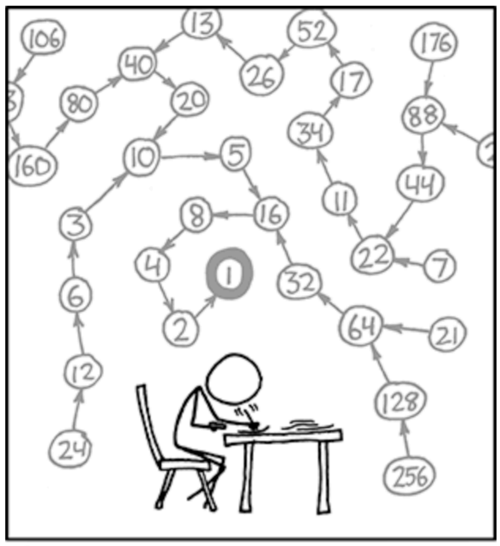
The equation $x^n + y^n = z^n$ has no integer solutions x, y, z with $xyz \neq 0$ and n is an integer > 2.

($n=2$ are pythagorean triples $3^2+4^2=5^2$)

Try some examples and there are no solutions so this lead to the conjecture which leads to the proof of the Theorem

Example: Collatz Conjecture

No counterexample found up to 5.48×10^{18}.



THE COLLATZ CONJECTURE STATES THAT IF YOU PICK A NUMBER, AND IF IT'S EVEN DIVIDE IT BY TWO AND IF IT'S ODD MULTIPLY IT BY THREE AND ADD ONE, AND YOU REPEAT THIS PROCEDURE LONG ENOUGH, EVENTUALLY YOUR FRIENDS WILL STOP CALLING TO SEE IF YOU WANT TO HANG OUT.

Note: There are other proof methods and it is not limited to the ones we covered so far. We will cover induction later and we've also discussed proof by pictures.