uniqueness proofs

Uniqueness Proofs

Claiming something is "unique" means there is only one thing of that type.

Proposition: There is a unique real number a such that $a > 0$ and $a^2 = 1$.

There are two claims here:

- There exists a real number a such that $a^2 = 1$ and $a > 0$.
- There is *only one* real number with these properties.

Uniqueness proofs

Proofs typically go like this.

Theorem: There exists a unique x such that $P(x)$ is true.

Proof: First, we show that there is an x such that $P(x)$ is true. Now suppose that u and v are two things such that $P(u)$ and $P(v)$ are true. Then we show that $u = v$.

Prop. There exists a unique a such that $a > 0$ and $a^2 = 1$.

Proof: First observe that $a = 1$ is greater than zero and $a^2 = 1 = 1^2$ satisfies $a^2 = 1$. So at least one a with desired property exists.

We show uniqueness. Suppose $a^2 = 1$. Then $a^2 - 1 = 0$ or $(a+1)(a-1) = 0$. Therefore $a = +1$ or $a = -1$. If $a > 0$, then $a = +1$ is the only solution.

More Euclid's Algorithm

Proposition: Suppose a and b are natural numbers. Then there exists a unique $d \in \mathbb{N}$ so that m is a multiple of d if and only if $m = ax + by$ for some $x, y \in \mathbb{Z}$.

Notice the logical structure here. We must show:

- there is (at least one) d that makes the if and only if statement "m is a multiple of d if and only if $m = ax + by$ for some $x, y \in \mathbb{Z}$" true.
- then show that there is *at most one* d that has this property.

Proposition: Suppose a and b are natural numbers. Then there exists a unique $d \in \mathbb{N}$ so that m is a multiple of d if and only if $m = ax + by$ for some $x, y \in \mathbb{Z}$.

① Show there is a d so that

m is a multiple of d

$\Downarrow$

$m = ax + by$

then

$m = ax + by$

$\Downarrow$

m is a multiple of d

② there is only one such.

Step 1A: Let $d = \gcd(a, b)$.

$1 = 7 + 3(-2)$
$5 = 7 \cdot 5 + 3(-10)$

The goal is to show that

$$d | m \Leftrightarrow m = ax + by \text{ for some } x, y \in \mathbb{Z}$$

- We will show that d makes the if and only if statement true.
- First we show that $d | m \implies m = ax + by$ for some x and y.
- Suppose that m is a multiple of d, so $m = dg$.
- We know that $d = ak + bl$, so $m = dg = a(gk) + b(gl)$.
- Choosing $x = gk$ and $y = gl$ we see that there exist x, y in $\mathbb{Z}$ so that $m = ax + by$

Step 1B:

Remember:

$d = \gcd(a, b)$

$$d | m \Leftrightarrow m = ax + by \text{ for some } x, y \in \mathbb{Z}$$

- Now we show that $m = ax + by$ for some $x, y \in \mathbb{Z}$ implies that $d|m$.
- We know that $a = ud$ and $b = vd$ for some u and v in $\mathbb{N}$.
- Therefore $m = udx + vdy = d(ux + vy)$ so m is a multiple of d.

Step 2A:

- Now we must show that $d = \gcd(a, b)$ is the *only* integer g that makes the if and only if statement

$$\underbrace{g}_{= d'} | m \Leftrightarrow m = ax + by \text{ for some } x, y \in \mathbb{Z}$$

of the theorem true. Our strategy is to suppose we have another integer d' that has this property, and then prove $d \geq d'$ and $d \leq d'$. So suppose that d' makes the if and only if statement true.

- Now we show $d' \leq d$.

$a = a \cdot 1 + b \cdot 0$
$\Rightarrow d' | a$

- The if and only if statement tells us that $d'|a$ since $a = a(1) + b(0)$ and $d'|b$ since $b = a(0) + b(1)$.

$b = a \cdot 0 + b \cdot 1$
$\Rightarrow d' | b$

- Therefore d' is a common divisor of a and b, and so $d' \leq d$.

since $d = \gcd(a,b)$

Step 2B:

- Next we show $d \leq d'$.
- Since $d'|d'$, we can find x and y so that $d' = \underline{ax + by}$.
- Since $a = ud$ and $b = vd$ for some integers u and v, we get $d' = d(ux + by)$ so $d|d'$ so $d' \geq d$.
- Combining Steps 2A and 2B we see that $\underline{d' = d}$.