Today: Prove that $\sqrt{2}$ is irrational.

- Proof by Contradiction, and Well-Ordering Principle.

From homework: Consider the function

$$f : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}$$
$$(a, b) \longmapsto \frac{a}{b}$$

Question: Is f injective?

Question: Is f surjective?

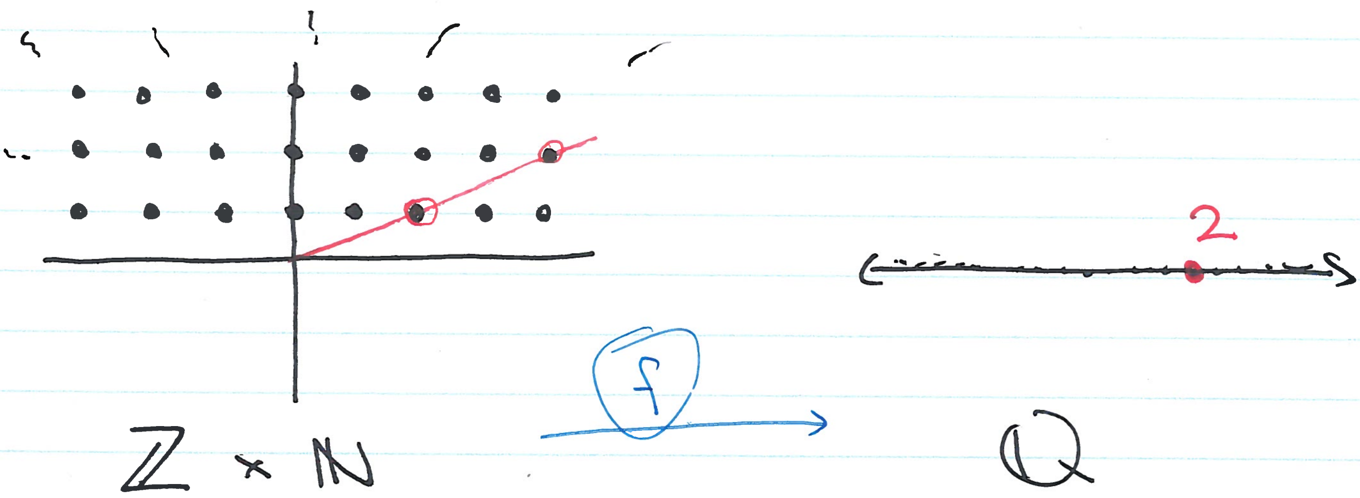
Surjective: Yes, because any rational number can be written as $\frac{a}{b}$, $a \in \mathbb{Z}$ and $b \in \mathbb{N}$.

Injective: No, for example,

$$f(10, 5) = \frac{10}{5} = 2$$
$$f(6, 3) = \frac{6}{3} = 2.$$

Note: The set $\mathbb{Z} \times \mathbb{N}$ is "bigger" than $\mathbb{Q}$.

Next week we will discuss sizes of infinite sets, and see $\mathbb{Z} \times \mathbb{N}$ and $\mathbb{Q}$ have the same size.



$$2 = \frac{2}{1} = \frac{4}{2} = \frac{6}{3} = \frac{8}{4} = \cdots$$

The <u>preimage</u> $f^{-1}(\{2\})$ = all points $(a,b) \in \mathbb{Z}\times\mathbb{N}$ on the line of slope $\frac{1}{2}$

<u>preimage</u> $f^{-1}(\{x\})$ = all points on the line of slope $\frac{1}{x}$

(In HW: equivalence relation on $\mathbb{Z}\times\mathbb{N}$.)

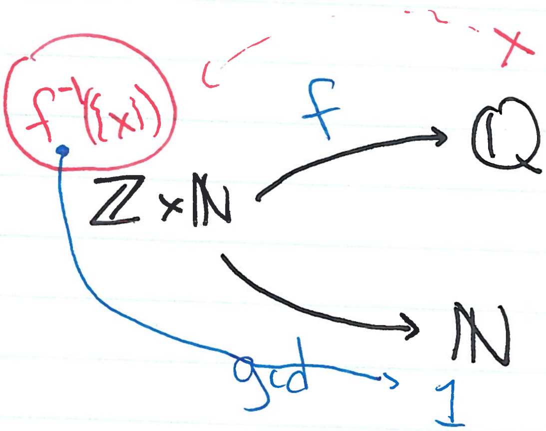
Consider the function

$$\text{gcd}: \mathbb{Z}\times\mathbb{N} \longrightarrow \mathbb{N}$$
$$(a,b) \longmapsto \gcd(a,b)$$

Proposition: For every $x \in \mathbb{Q}$, there exists a pair $(a,b) \in \mathbb{Z} \times \mathbb{N}$ such that

- $\frac{a}{b} = x$ (i.e. $f(a,b) = x$)
- $\gcd(a,b) = 1$.

Pf: We are saying
"$\forall x \in \mathbb{Q}$, $\exists (a,b) \in f^{-1}(\{x\})$ such that $\gcd(a,b) = 1$"



Consider the set of natural numbers

$$S = \{\gcd(a,b) : (a,b) \in f^{-1}(\{x\})\}.$$

S has a minimal element (WOP). Call it d, and suppose for a contradiction that $d \geq 2$.
Then there's a pair $(a,b) \in f^{-1}(\{x\})$ such that $\gcd(a,b) = d$.
But then, $\left(\frac{a}{d}, \frac{b}{d}\right) \in f^{-1}(\{x\})$. And $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
This shows $1 \in S$, which contradicts minimality of d. ∎

Theorem: $\sqrt{2}$ is irrational.

Proof:

> **Lemma:** Let n be an ~~natural number~~ integer. Then
> n^2 is even $\iff$ n is even.

Suppose $\sqrt{2}$ is rational. ← only assumption we made.

So $\exists\, a \in \mathbb{Z}$ and $\exists\, b \in \mathbb{N}$, s.t. $\sqrt{2} = \frac{a}{b}$.

uses our previous proposition → Without loss of generality, assume $\boxed{\gcd(a,b)=1.}$

$$\sqrt{2} = \frac{a}{b}$$

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2 \Rightarrow a^2 \text{ is even}$$

$$\Rightarrow a \text{ is even.}$$

So $\exists\, c \in \mathbb{Z}$, $\boxed{a = 2c.}$

$$2b^2 = (2c)^2 = 4c^2$$

$$b^2 = 2c^2 \Rightarrow b^2 \text{ is even}$$

$$\Rightarrow b \text{ is even}$$

→ It's impossible to have $2 \mid a$, $2 \mid b$, and $\gcd(a,b) = 1$.

Contradiction! $\rightarrow\leftarrow$.

Therefore, $\sqrt{2}$ is irrational. ∎

Note: Infinitely dividing 2's out from numerator & denominator is impossible! (Well-Ordering Principle)

(1) Exercise: Prove $\sqrt{3}$ is irrational. (Similar proof!)

(2) Exercise: If you try to prove $\sqrt{4}$ is irrational, which step fails?

(1) To prove $\sqrt{3}$ is irrational, use the following Lemma:

Lemma: $\forall n \in \mathbb{Z}$, $3 | n \iff 3 | n^2$

Pf: $\Rightarrow$: Suppose $3|n$. Then $\exists m \in \mathbb{Z}$ s.t. $n = 3m$.
Then $n^2 = 9m^2 = 3(3m^2)$ so $3 | n^2$.

$\Leftarrow$: We prove the contrapositive. Suppose $3 \nmid n$.
Then either $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$

- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1 \pmod 3$ so $3 \nmid n^2$
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 1 \pmod 3$ so $3 \nmid n^2$. ∎

Now the proof that $\sqrt{3}$ is irrational looks almost the same as the proof that $\sqrt{2}$ is irrational, but using the Lemma above.

(2) (Lemma: $\forall n \in \mathbb{Z}$, $4 | n \iff 4 | n^2$) is false!

Example, $n = 2$. Then ~~$4 \nmid n^2$ and $4 \nmid n$~~ $4 \nmid n$ and $4 | n^2$.

$\frac{a}{b} = \sqrt{4}$

Thus, when we go $a^2 = 4b^2 \Rightarrow a^2$ is divisible by 4,
we can't then say a is divisible by 4.