Q: Suppose there're 25 students in your discussion.

Which one is more likely?

✓ ① there're two students with the same birthday.

② everyone has different birthdays.

A proof is a finite list of logical deductions which establishes the truth of a statement.

1. Direct Proof

Goal: Prove $P \Rightarrow Q$.

Method: Assume P.

Deduce Q.

integers

E.g. $\boxed{\text{Def}}$ Given $a, b \in \mathbb{Z}$, $a \neq 0$, we say a **divides** b,

written $a | b$, if $\exists\, d \in \mathbb{Z}$, $ad = b$.

$\boxed{\text{Prop}}$ $\forall\, a, b_1, b_2 \in \mathbb{Z}$, if $a | b_1$ and $a | b_2$, then $a | b_1 - b_2$.

Pf: Let $a, b_1, b_2 \in \mathbb{Z}$.

Assume $a | b_1$ and $a | b_2$.

By definition, $\exists\, d_1, d_2 \in \mathbb{Z}$ such that

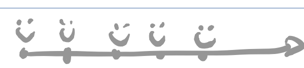
$ad_1 = b_1$, $ad_2 = b_2$.

Then, $b_1 - b_2 = ad_1 - ad_2 = a(d_1 - d_2)$.

By definition, $a | b_1 - b_2$.

$\square$

Rem. • To prove $\forall x, P(x)$,



pick an arbitrary c in the domain, and prove $P(c)$.

• To prove $\exists x, P(x)$,

find one element d in the domain and show $P(d)$.

2. Proof by Contraposition

Recall the contrapositive of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$.

Goal: Prove $P \Rightarrow Q$.

Method: Prove $\neg Q \Rightarrow \neg P$.

E.g. $\boxed{\text{Prop}}$ Let $n \in \mathbb{Z}$.

Prove that if n^2 is even, then n is even.

attempt direct proof: n^2 is even $\Rightarrow \exists k \in \mathbb{Z},\ n^2 = 2k$

$\Rightarrow n = \pm\sqrt{2k}$

???

Pf: Equivalent, we'll prove

n is odd $\Rightarrow n^2$ is odd.

Assume n is odd.

Then $n = 2k+1$ for some $k \in \mathbb{Z}$.

Thus, $n^2 = (2k+1)^2 = \underbrace{4k^2 + 4k}+1$

$= 2(2k^2+2k)+1$

By definition, n^2 is odd. $\square$

3. Proof by Contradiction

Goal: Prove P

Method: Assume $\neg P$.

Deduce $R \wedge \neg R$ for some R.

E.g. $\boxed{\text{Def}}$ A real number r is rational if there exist $p, q \in \mathbb{Z}$ with $q \neq 0$, such that $r = p/q$.

$\boxed{\text{Prop}}$: Let $\sqrt{2}$ be a solution to $x^2 = 2$. Then $\sqrt{2}$ is irrational.

Pf: Assume $\sqrt{2}$ is rational.

Let $p, q \in \mathbb{Z}$, $q \neq 0$, be such that $\sqrt{2} = \frac{p}{q}$.

Notice that we can pick p, q such that p, q don't have common divisors.

By the definition of $\sqrt{2}$,

$$(\sqrt{2})^2 = \left(\frac{p}{q}\right)^2 = \underbrace{\frac{p^2}{q^2} = 2}$$

$\Rightarrow p^2 = 2q^2 \Rightarrow p^2$ is even $\Rightarrow p$ is even.

By definition, $p = 2k$ for some $k \in \mathbb{Z}$.

Then $p^2 = (2k)^2 = \underbrace{4k^2 = 2q^2}$

$\Rightarrow 2k^2 = q^2$

$\Rightarrow q^2$ is even $\Rightarrow q$ is even.

Contradict with p, q having no common divisor,

$\Rightarrow \sqrt{2}$ must be irrational. $\square$

E.g. $\boxed{\text{Def.}}$ A **prime number** is a natural number greater than 1 whose only positive divisors are 1 and itself.

$\boxed{\text{Prop.}}$ There are infinite many prime numbers.

Pf: Assume there are finitely many primes $p_1, \dots, p_n$.

Consider $q = p_1 \cdots p_n + 1$. $\Rightarrow 1 = q - p_1 \cdots p_n$.

Since $q \neq p_i$ for $i = 1, \dots, n$, q is not prime.

Suppose p is a prime divisor of q.

Since $p \mid q$, $p \mid p_1 \cdots p_n$, thus $p \mid q - p_1 \cdots p_n$,

i.e. $p \mid 1$, contradiction.

Thus, there are infinitely many primes. $\square$

4. Miscellaneous

- To prove equivalence, i.e. $P \Leftrightarrow Q$, we show $P \Rightarrow Q$ and $Q \Rightarrow P$.

  Oftentimes, proof of equivalence is phrased as "if and only if" (iff).

- "without loss of generality, [assumption]" (WLOG) means the assumption that follows is chosen arbitrarily, narrowing down the statement to a particular case, but does not affect the validity of the proof in general.

E.g. $\boxed{\text{Prop}}$ Let $x, y \in \mathbb{Z}$. If (both xy and $x+y$ are even), then both x and y are even.

Pf: (contrapositive: either x is odd or y is odd $\Rightarrow$ either xy is odd or $x+y$ is odd).

WLOG, assume x is odd, i.e. $x = 2m+1$ for some $m \in \mathbb{Z}$.

Sometimes it's useful to divide up proof into exhaustive cases.

Pf (cont.): We want show either xy is odd or $x+y$ is odd.

Case 1: y is even

Then $y = 2n$ for some $n \in \mathbb{Z}$.

Hence $x+y = 2m+1+2n = 2(m+n)+1$ is odd.

Case 2: y is odd

Then $y = 2n+1$ for some $n \in \mathbb{Z}$.

Hence
$$\begin{aligned} xy &= (2m+1)(2n+1) \\ &= \underline{4mn + 2m + 2n} + 1 \\ &= 2(2mn+m+n)+1 \end{aligned}$$
is odd.

This proves the statement by contraposition. $\square$

- Constructive Existence Proofs:

Recall that to show "$\exists x\, P(x)$", find an element a such that $P(a)$ is true.

E.g. $\boxed{\text{Prop}}$ There exist irrational x, y such that x^y is rational.

Pf: Let $x = e$, $y = \ln 2$. Then $x^y = e^{\ln 2} = 2$. □

- Nonconstructive Existance Proof.

E.g. $\boxed{\text{Prop}}$ [There exist irrational x, y such that x^y is rational.] Q.

Pf: ① Assume $\sqrt{2}^{\sqrt{2}}$ is rational. ← P.

Then let $x = y = \sqrt{2}$ and we're done.

② Assume $\sqrt{2}^{\sqrt{2}}$ is irrational. $\neg P$.

Then $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.

we're done. □

$$\left.\begin{array}{l} P \Rightarrow Q, \\ \neg P \Rightarrow Q. \end{array}\right\} \underbrace{\underbrace{\neg P \vee P}_{T} \Rightarrow Q}$$

since implication is correct. and hypothesis is correct, we know the conclusion is correct

$\boxed{\text{WTS } P \Rightarrow Q}$

Assume P,

Goal: Prove Q.