Principle of Mathematical Induction

Suppose that $\forall n \in \mathbb{N}$, $S(n)$ is a logical statement, and that:

1) $S(1)$ is true, and
2) $\forall n \in \mathbb{N}$, $S(n) \Rightarrow S(n+1)$.

Then $S(n)$ is true for all $n \in \mathbb{N}$.

So, to prove that $S(n)$ is true, $\forall n \in \mathbb{N}$:

Base case

Prove that $S(1)$ is true.

Inductive step

Prove that, $\forall n \in \mathbb{N}$, $\underbrace{\text{if } S(n) \text{ is true}}_{\text{(inductive hypothesis)}}$ then $S(n+1)$ is true.

Conclude that $S(n)$ is true, $\forall n \in \mathbb{N}$.

Possible modifications:

- If we want to prove that $S(n)$ is true, $\forall n \geq b$, where $b \in \mathbb{Z}$, then for the base case we should prove that $S(b)$ is true.

- Sometimes you may need to establish more "base cases" to get the inductive step to work.

- For the inductive step, instead of proving

$$\left(\begin{array}{l} \forall n \in \mathbb{N}, \text{ if } S(n) \text{ is true,} \\ \quad \text{then } S(n+1) \text{ is true,} \end{array} \right) \quad \text{(weak induction)}$$

we could prove that

$$\left(\begin{array}{l} \forall n \in \mathbb{N}, \text{ if } S(m) \text{ is true, } \forall\, 1 \leq m \leq n, \\ \quad \text{then } S(n+1) \text{ is true.} \end{array} \right) \quad \text{(strong induction)}$$

Well-ordering principle

Suppose $A \subseteq \mathbb{N}$.

If $A \neq \emptyset$, then $\exists n \in A$ s.t. $\forall m \in A$, $m \geq n$.

(Every non-empty subset of $\mathbb{N}$ has a smallest element.)

Pf: Consider the contrapositive: (logically equiv.)

$\sim(\exists n \in A \text{ s.t. } \forall m \in A,\ m \geq n) \implies A = \emptyset$.

Equivalently:

$\forall n \in A, \exists m \in A \text{ s.t. } m < n \implies A = \emptyset$.

Suppose the statement on the left is true, and $\forall n \in \mathbb{N}$ let $S(n)$ be the statement that $n \notin A$. To show that $A = \emptyset$ is the same as showing that $\forall n \in \mathbb{N}$, $S(n)$ is true.

We proceed by (strong) induction:

Base case: If $1 \in A$ then, by assumption, $\exists m < 1$ s.t. $m \in A$. However $A \subseteq \mathbb{N}$, so this is impossible. Therefore $1 \notin A$, so $S(1)$ is true.

Inductive step: Suppose that $n \in \mathbb{N}$ and that $S(m)$ is true, $\forall\, 1 \le m \le n$. $(m \notin A,\ \forall\, 1 \le m \le n)$

If $n+1 \in A$ then, by assumption, $\exists\, m < n+1$ s.t. $m \in A$. But then it must be the case that $1 \le m \le n$, which is a contradiction.

Therefore $n+1 \notin A$, so $S(n+1)$ is true.

Conclusion: $\forall n \in \mathbb{N}$, $S(n)$ is true.

Therefore $A = \emptyset$. $\boxtimes$

Possible modifications

- Could assume that $A \subseteq \mathbb{Z}$, $A \neq \emptyset$, and that $\exists\, x \in \mathbb{R}$ s.t. $\forall n \in A$, $n \ge x$.

- Could assume that $A \subseteq \mathbb{Z}$, $A \neq \emptyset$, and that $\exists\, x \in \mathbb{R}$ s.t. $\forall n \in A$, $n \le x$, but then conclude that A has a largest element.

Division algorithm

Suppose that $a, b \in \mathbb{Z}$ and that $b \neq 0$. Then there exist unique integers q and r with

$$a = \underset{\text{(quotient)}}{q}\, b + \underset{\text{(remainder)}}{r} \quad \text{and} \quad 0 \leq r < |b|$$

Sketch of proof: (existence only)

Suppose $b > 0$. Consider the set

$$A = \{ n \in \mathbb{Z} : a - nb \geq 0 \}$$

Then: • $A \neq \emptyset$:

- if $a \geq 0$ then $a - 0 \cdot b = a \geq 0$, so $0 \in A$.
- if $a < 0$ then $a - ab = a(1-b) \geq 0$, so $a \in A$.

• $\forall n \in A,\ n \leq \frac{a}{b}$.

By the Well Ordering Principle:

$$\exists q \in A \text{ s.t. } \forall n \in A,\ n \leq q.$$

(cont. on next page)

Let $r = a - qb$. Then:

- $q \in A \Rightarrow r \geq 0$.
- If $r \geq b$ then

  $$a-(q+1)b = (a-qb)-b = r-b \geq 0$$

  $\Rightarrow q+1 \in A$, which is a contradiction.

  Therefore $r < b$.

Uniqueness: ... $\blacksquare$

gcd and lcm

If $a, d \in \mathbb{Z}$ with $d \neq 0$, we say that d divides a, and write $d \mid a$, if $\exists\, q \in \mathbb{Z}$ s.t. $a = qd$.
Otherwise we write $d \nmid a$.

Facts: Suppose $a, b \in \mathbb{Z} \setminus \{0\}$. Then:

- There is a unique $d \in \mathbb{N}$, called the greatest common divisor of a and b, with the following properties:

  i) $d \mid a$ and $d \mid b$. (common divisor)

  ii) If $e \in \mathbb{Z}$, $e \mid a$, and $e \mid b$, then $e \mid d$. (greatest)

  Notation: $d = \gcd(a, b) = (a, b)$.

  Abbreviations: gcd, gcf, hcf.

- There is a unique $\ell \in \mathbb{N}$, called the least common multiple of a and b, with the following properties:

  i) $a \mid \ell$ and $b \mid \ell$. (common multiple)

  ii) If $m \in \mathbb{Z}$, $a \mid m$, and $b \mid m$, then $\ell \mid m$. (least)

  Notation: $\ell = \operatorname{lcm}(a, b)$

  Abbreviations: lcm = lcd

- $|ab| = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$

Special case: If $\gcd(a,b)=1$ then $|ab| = \operatorname{lcm}(a,b)$.

(a and b are relatively prime).

Two ways to compute $\gcd(a,b)$:

- Factor a and b ... (no known "fast" algorithm)
- Use the Euclidean algorithm. (fast)

Observation: Suppose $a,b \in \mathbb{Z} \setminus \{0\}$ and write

$$a = qb + r, \quad q,r \in \mathbb{Z}, \quad 0 \le r < |b|.$$

Then $(a,b) = (b,r)$.

Pf: Follows from the facts that

$$(a,b) \mid a,b \Rightarrow (a,b) \mid a - qb = r \Rightarrow (a,b) \mid (b,r)$$

and that

$$(b,r) \mid b,r \Rightarrow (b,r) \mid qb + r = a \Rightarrow (b,r) \mid (a,b). \quad \blacksquare$$

Euclidean algorithm

Suppose $a, b \in \mathbb{Z} \setminus \{0\}$. Compute

$a = q_1 b + r_1$, $\quad q_1 \in \mathbb{Z}$, $\quad 0 \le r_1 < |b|$ $\quad$ (write $r_0 = |b|$)

$b = q_2 r_1 + r_2$, $\quad q_2 \in \mathbb{Z}$, $\quad 0 \le r_2 < r_1$

$r_1 = q_3 r_2 + r_3$, $\quad q_3 \in \mathbb{Z}$, $\quad 0 \le r_3 < r_2$

$\vdots \qquad \vdots$

$r_{n-1} = q_{n+1} r_n + r_{n+1}$, $\quad q_{n+1} \in \mathbb{Z}$, $\quad 0 \le r_{n+1} < r_n$

$r_n = q_{n+2} r_{n+1}$, $\quad q_{n+2} \in \mathbb{Z}$ $\quad$ (stop as soon as you get a remainder of 0).

Then $(a,b) = (b, r_1) = (r_1, r_2) = \cdots = (r_n, r_{n+1}) = r_{n+1}$.

Ex: $a = 218683$, $b = 215221$, compute (a,b).

$a = 1 \cdot b + 3462$ $\qquad$ $(q_1 = 1,\ r_1 = 3462)$

$b = 62 \cdot 3462 + 577$ $\qquad$ $(q_2 = 62,\ r_2 = 577)$

$3462 = 6 \cdot 577$ $\qquad$ ($q_3 = 6$, no remainder)

Conclusion: $(a,b) = 577$.

Note: $a = 379 \cdot 577$, $b = 373 \cdot 577$, so this problem is much more difficult to do by brute force factorization.

An important corollary:

Bézout's lemma: Suppose $a, b \in \mathbb{Z} \setminus \{0\}$ and let $d = \gcd(a,b)$.

Then $\{ak + b\ell : k, \ell \in \mathbb{Z}\} = \{qd : q \in \mathbb{Z}\}$.

In particular,

$$\exists\, k, \ell \in \mathbb{Z} \text{ s.t. } ak + b\ell = d.$$

How to find $k, \ell \in \mathbb{Z}$ s.t. $ak + b\ell = d$:

① Euc. alg.

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$
$$r_n = q_{n+2} r_{n+1}$$

② Reverse Euc. alg.

$$= ka + \ell b$$
$$= k_{n-1} b + \ell_{n-1} r_1$$
$$\vdots$$
$$= r_{n-1} - q_{n+1}(r_{n-2} - q_n r_{n-1}) = k_1 r_{n-2} + \ell_1 r_{n-1}$$
$$(a,b) = r_{n+1} = r_{n-1} - q_{n+1} r_n$$

Ex: $a = 218683$, $b = 215221$, $(a,b) = 577$.

$$a = 1 \cdot b + 3462$$
$$b = 62 \cdot 3462 + 577$$
$$3462 = 6 \cdot 577$$

$$= b - 62(a - b) = -62 \cdot a + 63 \cdot b$$
$$577 = b - 62 \cdot 3462$$

So $(a,b) = 577 = -62 \cdot a + 63 \cdot b$.

Fundamental Theorem of Arithmetic

A **prime number** is an integer $p>1$ whose only positive divisors are 1 and p.

Theorem (FTAr): If $n>1$ is an integer then there is a unique way of writing

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $k \in \mathbb{N}$, $p_1 < p_2 < \cdots < p_k$ are prime numbers, and $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$.

Useful facts:

- If p is a prime number, $a,b \in \mathbb{Z}$, and $p \mid ab$, then $p \mid a$ or $p \mid b$.
  (not true if $p > 1$ is not prime)

- Suppose that $p_1 < p_2 < \cdots < p_\ell$ are primes and that

$$a = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}, \qquad a_1, \ldots, a_\ell \geq 0,$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_\ell^{b_\ell}, \qquad b_1, \ldots, b_\ell \geq 0.$$

Then:

i) $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_\ell^{\min(a_\ell,b_\ell)}$

ii) $\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_\ell^{\max(a_\ell,b_\ell)}$