How induction works:

Let A be a set. To show that $A = \mathbb{N}$, we need two steps:

① Show that $1 \in A$

② Show that if $k \in A$, then $k+1 \in A$.

Together, ① and ② implies that $A = \mathbb{N}$.

How strong induction works:

Let A be a set. To show that $A = \mathbb{N}$, we need two steps:

① Show that $1 \in A$.

② Show that if $\{1, 2, \ldots, k\} \subseteq A$, then $k+1 \in A$.

Together, ① and ② implies that $A = \mathbb{N}$.

Obs: we can adapt proofs by induction or strong induction to deal with cases where the inductive step is valid only for integers greater than a particular integer.

Applications of strong induction:

For the first application, we need the definition of a prime number.

Definition: We say that a natural number $n > 1$ is a prime number if n is only divisible by 1 and itself.

In other words,

$$n = a \cdot b \ (a, b \in \mathbb{N}) \Rightarrow a = 1 \text{ or } b = 1.$$

Theorem: Every integer greater than 1 can be written as the product of primes.

proof:

Define $P(n) =$ " n can be written as the product of primes "

Define $P(n)$ ...

and set

$$A = \{ n \in \mathbb{N} : n \geq 2 \text{ and } P(n) \text{ is true} \}$$

Note $P(2)$ is true : 2 can be written as the product of one prime, itself. This is the basis step.

Inductive step : Suppose that $\{2, \dots, k\} \subseteq A$.

Now, we must show that $k+1 \in A$. That is, $P(k+1)$ is true.

We have two cases :

① $k+1$ is prime.

In this case we are done because $k+1$ can be written as the product of one prime, itself.

② If $k+1$ is not prime, then $\exists\, a, b \in \mathbb{N} \setminus \{1\}$ such that

$$k+1 = a \cdot b$$

As $a, b \geq 2$, we have $a, b \leq \frac{k+1}{2} \leq k$, and hence

we can apply our induction hypothesis.

As $\{2, \dots, k\} \subseteq A$, we have that $\{a, b\} \subseteq A$

and hence a and b can be written as a product of primes. This shows that $k+1$ is a product of primes.

We conclude that

① $2 \in A$

② If $\{2, 3, \dots, k\} \subseteq A$, then $k+1 \in A$.

Together, ① and ② imply that $A = \mathbb{N} \setminus \{1\}$. ∎

Problem : Consider a game in which two players take turns remove any positive number of matches they want from one or removing any pos

two piles of matches. The player who removes the last match wins the game. Show that if two players contain the same number of matches initially, the second player can always guarantee a win.

Solution :

For $n \in \mathbb{N}$, let

$P(n) =$ "Player 2 wins if both piles have size n".

Define

$A = \{ n \in \mathbb{N} : P(n) \text{ is true} \}$

Note that $P(1)$ is true, and hence $1 \in A$.

Now, suppose that $\{1, 2, \dots, k\} \subseteq A$.

We will show that $k+1 \in A$.

Suppose that player 1 removes r matches from some pile, where $1 \leq r \leq k+1$.

Without loss of generality, we can assume that player 1 took r matches from pile 1.

Now the second player can remove r matches from pile 2.

This way, we arrive in a situation where we have two piles of length $k+1-r \leq k$ and player 1 plays next. By induction hypothesis, player 2 wins this game. Therefore, $P(k+1)$ is true, and hence $k+1 \in A$.

We conclude that $A = \mathbb{N}$. $\blacksquare$

<u>Definition</u>: We say that a set A has a least element if $\exists\, a \in A$ such that $a \leq b \ \forall\, b \in A$.

<u>THE WELL-ORDERING PRINCIPLE</u>: Every set $A \subseteq \mathbb{N}$ has a least element.

Application of the well-ordering principle:

<u>Theorem</u>: If $a \in \mathbb{Z}, d \in \mathbb{N}$, then there are unique integers q and r with $0 \leq r < d$ and $a = dq + r$.

<u>proof</u>: Define $S = \{a - dq : q \in \mathbb{Z}\} \cap (\{0\} \cup \mathbb{N})$.

Note that S is non-empty. (make $-dq$ large).

By the well-ordering principle, S has a least element, let us say $r = a - dq_0$.

<u>Claim</u>: $r < d$.

<u>proof of claim</u>: Suppose for contradiction that $r \geq d$.

Then,
$$r > r - d = a - d(q_0 + 1) \geq 0$$

This contradicts the choice of r. $\blacksquare$

As $0 \leq r < d$, we show the existence.

The proof of uniqueness is left as an exercise $\blacksquare$