1. What is the Principle of Mathematical Induction? Suppose P(n) is a predicate with variable n. We may form the statement

(*) 'for any $n \in \mathbb{N}$, P(n) holds.'

This eives

that we

Principle

Mathematical

Induction

One standard method which may help proving such a statement is 'mathematical induction'.

It is based on the validity of (First) Principle of Mathematical Induction, in its 'usual' formulation:

Let P(n) be a predicate with variable n. Suppose the statement P(0) is true. Further suppose that for any $k \in \mathbb{N}$, if the statement P(k) is true then the statestatement ment P(k+1) is true. are reterring Then the statement P(n) is true for any $n \in \mathbb{N}$. to as the This is the conclusion in the statement

2. Format of a mathematical induction argument.

General scheme in the application of the Principle of Mathematical Induction to prove (\star) :

- Step (0). Identify P(n) and write it down explicitly.
- Step (1). Prove the statement P(0). (This is the 'initial step argument'.)
- Step (2). Assume the statement P(k) to be true. (This is called the induction assumption.) Prove the statement P(k + 1) under this assumption. (This is the 'induction argument'.)
- Step (3). Declare that according to the Principle of Mathematical Induction, P(n) is true for any $n \in \mathbb{N}$.

Theoretical support for this scheme?

What does the Principle of Matheamtical Induction say, really?

Let P(n) be a predicate with variable n.

Suppose the statement P(0) is true.

Further suppose that for any $k \in \mathbb{N}$, if the statement P(k) is true then the statement P(k+1) is true.

Then the statement P(n) is true for any $n \in \mathbb{N}$.

3. Simple examples in mathematical induction.



(b) Statement (B).

 $n^3 - n$ is divisible by 3 for any $n \in \mathbb{N}$. **Proof of Statement (B)**.

- · For any neW, dente by P(n) the proportion 'n -n is divisible by 3. · Ask: Is Pros true?] $0^{\circ} - 0 = 0 = 0.3$ DEK. Then 0³-0 is divisible by 3. Therefore P(0) is true.
- · Let KEN. Suppose P(k) is true. Then k'-k is divisible by 3. Ask: Is P(k+1) true under the assumption that P(k) is true, as stated above? We prove that P(k+1) is true: * By definition, there exits some $2 \in \mathbb{Z}$ such that $k^3 - k = 3q$. We have $(k+1)^{3} - (k+1) = ... = (k^{3} - k) + 3k^{2} + 3k = 3(9+k^{2}+k).$ Also note that g+k²+k eZ. [why? Detail?] Then $(k+1)^3 - (k+1)$ is divisible by 3. Hence P(k+1) is true. · By the Principle of Mathematical Induction, P(n) is true for any nell.

4. Mathematical Induction not 'starting from 0'?

There is nothing sacred about the number 0 in mathematical induction.

The initial step in an argument by mathematical induction may be concerned with any number other than 0.

(VPMI) Principle of Mathematical Induction, (variant of its 'usual' formulation):

Let P(n) be a predicate with variable n. Let $N \in \mathbb{Z}$.

Suppose the statement P(N) is true.

Further suppose that for any $k \in [N, +\infty)$, if the statement P(k) is true then the statement P(k+1) is true.

Then the statement P(n) is true for any $n \in [N, +\infty)$.

Remark. $[N, +\infty)$ is defined to be the set $\{m \in \mathbb{Z} : m \ge N\}$.

Theorem (1). The statements (UPMI), (VPMI) are logically equivalent to each other.

Further Remark.

What we have just seen is a particular instance of a more general situation.

Suppose T(x) is a predicate with variable x.

Suppose W is a set which may be regarded as a 'copy' of N, in the sense that we may label exhaustively and without repetition the elements of S as x_0, x_1, x_2, \cdots , we may form the predicate $T(x_n)$ with variable n, which we now denote by T'(n).

The statement

(†) 'for any
$$x \in W$$
, $T(x)$ holds'

is equivalent to

 (\dagger') 'for any $n \in \mathbb{N}$, T'(n) holds.'

Hence we may prove (\dagger) by applying mathematical induction to prove (\dagger') .

- 5. Further examples in mathematical induction.
 - (a) Statement (C). $\frac{(2n)!}{(n!)^2} > \frac{4^n}{n+1} \text{ for any } n \in \mathbb{N} \setminus \{0, 1\}.$ Proof of Statement (C).
 - For any $n \in \mathbb{N} \setminus \{0, 1\}$, denote by P(n) the proposition

$$\frac{(2n)!}{(n!)^2} > \frac{4^n}{n+1}$$

• Note that

$$\frac{(2\cdot 2)!}{(2!)^2} = \frac{24}{4} = 6 > \frac{16}{3} = \frac{4^2}{2+1}.$$

Then P(2) is true.

• Let $k \in \mathbb{N} \setminus \{0, 1\}$. Suppose P(k) is true. Then $\frac{(2k)!}{(k!)^2} > \frac{4^k}{k+1}$.

 $\begin{array}{c} \hline Roughwork. \\ \hline Ask: How to deduce <math>P(k+1)$ from $P(k)? \\ \hline Ask: How to deduce <math>P(k+1)$ from $P(k)? \\ \hline Further ark: Ang 'friendly' reformulation of <math>P(k), P(k+1)? \\ \hline Answer: P(k) is the same as <math>\frac{(k)!}{(k!)^2} \cdot \frac{k+1}{4^k} > 1 \\ \hline P(k+1) is the same as \dots ??? \\ \hline We prove that <math>P(k+1)$ is true: $\dots \end{array}$ $= \frac{(2k+2)(2k+1)}{(k+1)^2} \cdot \frac{(2k)!}{(k!)^2} \cdot \frac{k+1}{4k} \cdot \frac{k+2}{4(k+1)}$ $\frac{(2k)!}{(k!)^2} \cdot \frac{k+1}{4^k} \cdot \frac{(2k+1)(k+2)}{2(k+1)^2}$ $\frac{(k+1)(k+2)}{2(k+1)^{2}} = \frac{2k^{2}+5k+2}{2k^{2}+4k+2} > |.$ Then $\frac{[2(k+1)]!}{[(k+1)!]^{2}} > \frac{4^{k+1}}{(k+1)+1}$ Hence P(k+1) is true.

• By the Principle of Mathematical Induction, P(n) is true for any $n \in \mathbb{N} \setminus \{0, 1\}$.

(b) Statement (D).

For any $n \in [[8, +\infty)$, there exist some $u, v \in \mathbb{N}$ such that n = 3u + 5v. **Proof of Statement (D)**.

- For any nE [[8, +00), dente by P(n) the proportion that there exit some u, vEN such that n=3u+5v.
- · Note that IEN and 8=3.1+5.1. Then P(8) is true.
- · Let k ∈ [[8, +∞). Suppose P(k) is true. Then there exit some u, v ∈ M such that k=3u+5v.

We hope to deduce P(k+1): There exist some s,tein such that k+1 = 3s+5+. Ask: What to do to attain this objective?

Roughwork. Ask: Is the equality below possible? Try: k+1=3(5+5) Expressions k+1=3u+5v+1 k+1=3u+5v+1 autbv+c aut by +c with a, b, ce] = ... = 3(u+2)+5(v-1)Is it 'good ? Yes when v≥1. But what if V=0? When v=0, k=3u. Then u=3, and k+1=3u+1=..=3(u-3)+5.2. Note that V=0 or V≥1. * (Case 1). Suppose V=0. Then k=3u. Since k=8, we have u=3. Then u-3EN. Now k+1= 3n+1= 3(n-3)+5.2. (Note that 2EN.) * (Case 2). Suppose V≥1. Then V-IEN. Since NEW, we have ut 2EN. Nor k+1 = 3u+5v+1 = 3(u+2)+5(v-1). three in any case P(k+1) is true. · By the Principle of Mathematical Induction, P(n) is true for any nE[8, +00). I

- (c) Statement (E). (One of Weierstrass's Product Inequalities.) Let $n \in \mathbb{N} \setminus \{0, 1\}$. Suppose $b_1, b_2, \dots, b_n \in (0, 1)$. Then $(1-b_1)(1-b_2) \dots (1-b_n) > 1 - (b_1 + b_2 + \dots + b_n)$. Proof of Statement (E).
 - For any $n \in \mathbb{N} \setminus \{0, 1\}$, denote by P(n)the following proposition: Suppose $b_1, b_2, \cdots, b_n \in (0, 1)$. Then $(1-b_1)(1-b_2) \cdot \ldots \cdot (1-b_n)$ > $1 - (b_1 + b_2 + \dots + b_n).$ · Suppose a, b E (0,1). Then (1-a)(1-b) = 1-a-b+ab= 1-(a+b) + ab > 1-(a+b) + o = 1-(a+b). It follows that P(2) is true. • Let $k \in \mathbb{N} \setminus \{0, 1\}$. Suppose P(k) is true. (Therefore, for any C, C, ..., CKE(0,1), $(1-c_1)(1-c_2)\cdots(1-c_k)$ $> |-(c_1+c_2+...+c_k)$)

We prove that P(k+1) is true: Suppose b, b, ..., bk, bk+1 € (0,1). Then $(|-b_1)(|-b_2) \cdot \dots \cdot (|-b_k)(|-b_{k+1})$ $> [1-(b_1+b_2+...+b_k)](1-b_{k+1})$ = $1 - (b_1 + b_2 + ... + b_k) - b_{k+1} + (b_1 + b_2 + ... + b_k) b_{k+1}$ > $1 - (b_1 + b_1 + \dots + b_k + b_{k+1}) + 0$ (Why?) = 1- (b, +b2+...+b++b+++) Hence P(k+1) is true.

• By the Principle of Mathematical Induction, P(n) is true for any $n \in \mathbb{N} \setminus \{0, 1\}$.

(d) Statement (F).

Let p be a prime number. Let $n \in \mathbb{N} \setminus \{0, 1\}$. Let $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Suppose $a_1 a_2 \dots a_n$ is divisible by p. Then at least one of a_1, a_2, \dots, a_n is divisible by p.

Remarks.

- Euclid's Lemma is tacitly assumed here in the argument: Let $h, k \in \mathbb{Z}$, and p be a prime number. Suppose hk is divisible by p. Then at least one of h, k is divisible by p.
- The statement to be proved may be thought of as a generalization of Euclid's Lemma from the situation for products of two integers to that for any finite products of integers.

Proof of Statement (F). Exercise.

6. Why is the Principle of Mathematical Induction true?

The validity of the Principle of Mathematical Induction rests on something which is intuitively so obvious that we would have never doubted since childhood:

• There is a smallest number in each (non-empty) collection of natural numbers.

We proceed to formulate this 'intuitively obvious' 'fact' in precise mathematical language. **Definition.**

Let T be a subset of \mathbb{Z} , and $\lambda \in T$.

 λ is said to be a least element of T if for any $x \in T$, $\lambda \leq x$.

Well-ordering Principle for Integers (WOPI).

Let T be a non-empty subset of \mathbb{N} . T has a least element.

Theorem (2).

The Principle of Mathematical Induction (UPMI) is logically equivalent to the Wellordering Principle for Integers (WOPI).

7. Second Principle of Mathematical Induction.

The statement below is known as the **Second Principle of Mathematical Induc-**tion (PMI2):

Let Q(n) be a predicate with variable n.

Suppose the statement Q(0) is true.

Further suppose that for any $k \in \mathbb{N}$, if the statements $Q(0), Q(1), \dots, Q(k)$ are true then the statement Q(k+1) is true.

Then the statement Q(n) is true for any $n \in \mathbb{N}$.

Theorem (3).

The (First) Principle of Mathematical Induction (UPMI) is logically equivalent to the Second Principle of Mathematical Induction (PMI2).

8. Principle of Mathematical Induction in set language.

The Principle of Mathematical Induction (UPMI) can be re-formulated in terms of set equality and subset relations.

(SPMI). Principle of Mathematical Induction, (set-theoretic formulation). Let S be a subset of \mathbb{N} .

Suppose $0 \in S$. Further suppose that for any $k \in \mathbb{N}$, if $k \in S$ then $k + 1 \in S$. Then $S = \mathbb{N}$.

Theorem (4).

The statements (UPMI), (SPMI) are logically equivalent to each other.

Theorem (4).

The statements (UPMI), (SPMI) are logically equivalent to each other.

Proof of Theorem (4).

Argument for '(SPMI) \Longrightarrow (UPMI)':

Assume (SPMI) holds:

* Let S be a subset of N. Suppose $0 \in S$. Further suppose that for any $k \in \mathbb{N}$, if $k \in S$ then $k + 1 \in S$. Then $S = \mathbb{N}$.

[We want to deduce from this assumption '(SPMI) holds' that (UPMI) holds.]

Let P(n) be a predicate with variable n. Suppose the statement P(0) is true. Further suppose that for any $k \in \mathbb{N}$, if the statement P(k) is true then the statement P(k+1)is true. [We want to deduce, by applying (SPMI), that for any $n \in \mathbb{N}$, the statement P(n) is true.]

Define $S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$. [We now proceed to prove that $S = \mathbb{N}$.]

• Since the statement P(0) is true, we have $0 \in S$. Pick any $k \in \mathbb{N}$. Suppose $k \in S$. Then (by the definition of S) the statement P(k) is true. Since P(k) is true, P(k+1) is also true. Therefore (by the definition of S) we have $k + 1 \in S$.

Now, by (SPMI), $S = \mathbf{N}$.

It follows that for any $n \in \mathbb{N}$, the statement P(n) is true.

Theorem (4).

The statements (UPMI), (SPMI) are logically equivalent to each other.

Proof of Theorem (4). (Cont'd.)

Argument for '(UPMI) \Longrightarrow (SPMI)':

Assume (UPMI) holds:

* Let P(n) be a predicate with variable n. Suppose the statement P(0) is true. Further suppose that for any $k \in \mathbb{N}$, if the statement P(k) is true then the statement P(k+1) is true. Then the statement P(n) is true for any $n \in \mathbb{N}$.

[We want to deduce from this assumption '(UPMI) holds' that (SPMI) holds.] Let S be a subset of N. Suppose $0 \in S$. Further suppose that for any $k \in \mathbb{N}$, if $k \in S$ then $k + 1 \in S$. [We want to deduce, by applying (UPMI), that $\mathbb{N} \subset S$.]

• For any $n \in \mathbb{N}$, denote by P(n) the proposition $n \in S$. [We now proceed to apply mathematical induction to prove that for any $n \in \mathbb{N}$, P(n) is true.] By assumption, $0 \in S$. Then P(0) is true.

Let $k \in \mathbb{N}$. Suppose P(k) is true. Then $k \in S$. By the assumption on S, since $k \in S$, we also have $k + 1 \in S$. Therefore P(k + 1) is true.

By the Principle of Mathematical Induction, P(n) is true for any $n \in \mathbb{N}$.

We have verified that every element of \mathbb{N} is an element of S. Then $\mathbb{N} \subset S$. By definition $S \subset \mathbb{N}$. Hence $S = \mathbb{N}$. The Second Principle of Mathematical Induction (UPMI) can also be re-formulated in terms of set equality and subset relations.

(SPMI2). Second Principle of Mathematical Induction, (set-theoretic formulation).

Let U be a subset of N.

Suppose $0 \in U$.

Further suppose that for any $k \in \mathbb{N}$, if $0, 1, 2, \dots, k \in U$ then $k + 1 \in U$. Then $U = \mathbb{N}$.

Theorem (5).

The statements (PMI2), (SPMI2) are logically equivalent to each other. **Proof of Theorem (5).** Exercise. (The argument is similar to that for Theorem (4).)

9. Theorem (6).

The Well-ordering Principle for integers (WOPI), the (set-theoretic formulation of the) Principle of Mathematical Induction (SPMI), the (set-theoretic formulation of the) Second Principle of Mathematical Induction (SPMI2) are logically equivalent.

Outline and ideas on proof of Theorem (6).

Argument for '(WOPI) \Longrightarrow (SPMI)':

• Suppose the statement (WOPI) holds.

Let T be a subset of N. Suppose $0 \in T$. Further suppose that for any $n \in \mathbb{N}$, if $k \in T$ then $k + 1 \in T$.

By definition, $T \subset \mathbb{N}$. We verify that $\mathbb{N} \subset T$, with the method of proof by contradiction.

[*Idea.* Suppose it were true that $\mathbb{N} \not\subset T$. We look for a contradiction.

By assumption, there would exist some $x_0 \in \mathbb{N}$ such that $x_0 \notin T$.

Define $S = \{x \in \mathbb{N} : x \notin T\}$. Since $x_0 \in S$, we would have $S \neq \emptyset$.

(WOPI) would tell us that S had a least element, say, λ . By studying the number λ , we will come to a desired contradiction.

We will be forced to conclude that $\mathbb{N} \subset T$ in the first place.]

Since $T \subset \mathbb{N}$ and $\mathbb{N} \subset T$, we have $T = \mathbb{N}$.

It follows that the statement (SPMI) holds.

Theorem (6).

The Well-ordering Principle for integers (WOPI), the (set-theoretic formulation of the) Principle of Mathematical Induction (SPMI), the (set-theoretic formulation of the) Second Principle of Mathematical Induction (SPMI2) are logically equivalent.

Outline and ideas on proof of Theorem (6).

Argument for '(SPMI) \Longrightarrow (SPMI2)':

• Suppose that the statement (SPMI) holds.

Let U be a subset of N. Suppose that $0 \in U$. Further suppose that for any $k \in \mathbb{N}$, if $\llbracket 0, k \rrbracket \subset U$ then $k + 1 \in U$.

By definition, $U \subset \mathbb{N}$. We verify that $\mathbb{N} \subset U$:

```
[Idea. Define T = \{x \in \mathbb{N} : [[0, x]] \subset U\}.
Apply (SPMI) to deduce that T = \mathbb{N}.
Now ask: Is it true that every element of T an element of U? If yes, then it follows that \mathbb{N} \subset U, and furthermore \mathbb{N} = U.]
```

It follows that the statement (SPMI2) holds.

Theorem (6).

The Well-ordering Principle for integers (WOPI), the (set-theoretic formulation of the) Principle of Mathematical Induction (SPMI), the (set-theoretic formulation of the) Second Principle of Mathematical Induction (SPMI2) are logically equivalent.

Outline and ideas on proof of Theorem (6).

Argument for '(SPMI2) \Longrightarrow (WOPI)':

• Suppose that the statement (SPMI2) holds.

Let S be a non-empty subset of \mathbb{N} . We verify that S has a least element with the method of proof by contradiction:

 $[\mathit{Idea.}\$ Suppose it were true that S did not have a least element. We look for a contradiction.

Define $U = \mathbb{N} \setminus S$.

We verify that $0 \in U$, and that for any $k \in \mathbb{N}$, if $\llbracket 0, k \rrbracket \subset U$ then $k + 1 \in U$.

(SPMI2) would then imply that $U = \mathbb{N}$. It would then follow that $S = \emptyset$: this is the desired contradiction.]

It follows that the statement (WOPI) holds.

- 10. Further examples of statements which may be proved using mathematical induction.
 - (a) **Binomial Theorem for numbers.**

Let a, b be any numbers. For any $n \in \mathbb{N}$,

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots$$
$$+ \binom{n}{k}a^{n-k}b^k + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

(b) Leibniz's Rule (on repeated differentiation for products of functions).

Suppose g, h are real-valued functions of one real variable which are n-times differentiable at a. Then $g \cdot h$ is n-times differentiable at a and

$$(g \cdot h)^{(n)}(a) = g(a)h^{(n)}(a) + {\binom{n}{1}}g'(a)h^{(n-1)}(a) + {\binom{n}{2}}g''(a)h^{(n-2)}(a) + \cdots + {\binom{n}{k}}g^{(k)}(a)h^{(n-k)}(a) + \cdots + {\binom{n}{n-1}}g^{(n-1)}(a)h'(a) + g^{(n)}(a)h(a).$$

(c) Remainder Theorem and Factor Theorem 'combined'

Let $n \in \mathbb{N} \setminus \{0\}$. Let f(x) be a polynomial of degree n. Suppose α is a number. Then there exists some unique polynomial g(x) of degree n - 1 such that

$$f(x) = (x - \alpha)g(x) + f(\alpha)$$

as polynomials.

Remark. The Remainder Theorem and the Factor Theorem that you learnt in school maths are immediate consequences of this result:

• Remainder Theorem.

Let f(x) be a polynomial. Let α be a number. The remainder of f(x) upon division by $x - \alpha$ is $f(\alpha)$.

• Factor Theorem.

Let f(x) be a polynomial. Let α be a number. f(x) is divisible by $x - \alpha$ iff $f(\alpha) = 0$.

$(d) \ {\bf Generalized \ Triangle \ Inequality \ (on \ the \ complex \ plane)}.$

Let
$$n \in \mathbb{N} \setminus \{0, 1\}$$
. Suppose $\mu_1, \mu_2, \cdots, \mu_n \in \mathbb{C}$. Then $\left| \sum_{j=1}^n \mu_j \right| \le \sum_{j=1}^n |\mu_j|$.

(e) Existence Theorem for row equivalence to reduced row echelon forms.

Let p, q be positive integers. Suppose A is a $(p \times q)$ -matrix with real entries. Then there exists some $(p \times q)$ -matrix with real entries B such that B is a reduced row echelon form and A is row equivalent to B.

Remark. The corresponding 'uniqueness result' can also be proved with the help of mathematical induction.

(f) Fundamental Theorem of Arithmetic.

Let $n \in \mathbb{N} \setminus \{0, 1\}$. The statements below hold:

(1) n is a prime number or a product of several prime numbers.

(2) Let $p_1, p_2, \dots, p_s, q_1, q_2, \dots, q_t$ be prime numbers. Suppose $0 < p_1 \le p_2 \le \dots \le p_s$ and $0 < q_1 \le q_2 \le \dots \le q_t$. Further suppose $n = p_1 p_2 \cdot \dots \cdot p_s$ and $n = q_1 q_2 \cdot \dots \cdot q_t$. Then s = t and $p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$.