Some Proof Techniques.

Kin-Ma Ch

△Proof by contradiction

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

Pf. Let $\sqrt{2} = \frac{m}{n}$, where $m \geq 1$ and $n \geq 1$.

We assume that m and n are not both even. (For otherwise, ...)

$$\sqrt{2} = \frac{m}{n} \Rightarrow 2n^2 = m^2$$

$$\Rightarrow m^2 \text{ is even}$$

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

Let $m = 2k$

$$2n^2 = (2k)^2 = 4k^2$$

$$n^2 = 2k^2$$

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

A contradiction.

We conclude that $\sqrt{2}$ is irrational.

△ Nonconstractive proofs

Kun-Mao Chao

Prove that $\exists$ irrational numbers x and y such that

x^y is rational, i.e., $x^y \in \mathbb{Q}$.

Proof. If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, we are done. $(x=\sqrt{2}, y=\sqrt{2})$

Otherwise, $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$. $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$.

(x = $\sqrt{2}^{\sqrt{2}}$, y = $\sqrt{2}$) #

You may use $\sqrt{3}^{\sqrt{3}}$, ... as well.

△ Proof by Induction

Kin-Man Cha

Prove that for any finite set A, $|2^A| = 2^{|A|}$.

e.g.

$$|2^{\{b,d,f\}}| = |\{\phi, \{b\}, \{d\}, \{f\}, \{b,d\}, \{b,f\}, \{d,f\}, \{b,d,f\}\}| = 8 = 2^3 = 2^{|\{b,d,f\}|}$$

proof.

Basis Step. $|A| = 0 \Rightarrow A = \phi$

$$|2^A| = |\{\phi\}| = 1 = 2^0 = 2^{|A|}.$$

Induction Hypothesis.

Suppose that $|2^A| = 2^{|A|}$ for $|A| \le n$.

Induction Step.

Let $|A| = n+1$, and $a \in A$.

$B = A - \{a\} \Rightarrow |B| = n$

$|2^B| = 2^{|B|} = 2^n$ ← $|2^B|$

$2^A = 2^B \cup \{C \cup \{a\} : C \in 2^B\}$

$|2^A| = 2^n + 2^n = 2^{n+1} = 2^{|A|}$ Q.E.D.

Kuo-Mens Chen

The pigeon hole principle.

Thm. Let n be a positive number. Every sequence of n^2+1 distinct real numbers contains a subsequence of length $n+1$ that is either increasing or decreasing.

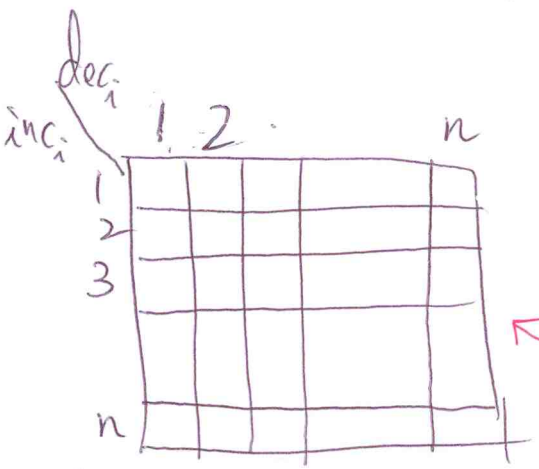
e.g. $(18, 5, 20, 8, 19)$

$(a_1, a_2, \cdots, a_{n^2+1})$

inc_i: the length of the longest increasing subsequence starting at a_i.

dec_i: " " decreasing " "

Assume that $inc_i \le n$ & $dec_i \le n$.



(pigeons) n^2+1 numbers

(pigeon holes) n^2 buckets

$\exists\, i<j$ s.t. $inc_i = inc_j$, $dec_i = dec_j$

$\cdots, a_i, \cdots, a_j \cdots$

If $a_i < a_j \Rightarrow inc_i \ge 1 + inc_j$

If $a_i > a_j \Rightarrow dec_i \ge 1 + dec_j$.

Kuan-Mao Chao

A is finite if $\exists$ a bijection function $f: A \mapsto \{1, 2, \cdots, n\}$ for some $n \in N$.

If A is not finite, it is infinite.

A is countably infinite if $\exists$ a bijection function $f: A \mapsto N$. [Note that $N = \{0, 1, 2, \cdots\}$ in this book.]

A is countable if it is finite or countably infinite.

Eg. The set of NTUCSIE teachers and students is countable. [finite].

The set of positive even numbers is countable. [$f(2)=0$, $f(4)=1$, $\cdots$, $f(a)=\frac{a}{2}-1$, $\cdots$]

The set of positive rational numbers is countable. [Why? Give it a try before you turn to the next page.]

Kan Hao Chan

△ Proof by Enumeration

The set of positive rational numbers is countable.

Let's count.

$\frac{1}{1}$

$\frac{1}{2}, \frac{2}{1}$

$\frac{1}{3}, \frac{2}{2}, \frac{3}{1}$

$\frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}$

$\vdots$

Since there are duplicated rational numbers, you might want to skip counting $\frac{1}{i}$ if $\gcd(i,j) \neq 1$.

$\frac{1}{i} \leftarrow ? \sum_{x=0}^{i+j-2} x + (j-1)$

$= \frac{(i+j-2)(i+j-1)}{2} + (j-1)$

Let A, B, C be countable sets. $A = \{a_0, a_1, a_2, \cdots\}$, $B = \{b_0, b_1, b_2, \cdots\}$, $C = \{c_0, c_1, c_2, \cdots\}$.

$A \cup B \cup C$ is countable.

A $\cdot a_0$ 0 $\cdot a_1$ 3 $\cdot a_2$ 6 . . .

B $\cdot b_0$ 1 $\cdot b_1$ 4 $\cdot b_2$ 7 . . .

C $\cdot c_0$ 2 $\cdot c_1$ 5 $\cdot c_2$ 8 . . .

$N \times N$ or N^2 is countable.

Kun-Mao Chao

$(0,0)^0$

$(0,1)^1\ (1,0)^2$

$(0,2)^3\ (1,1)^4\ (2,0)^5$

$(0,3)^6\ (1,2)^7\ (2,1)^8\ (3,0)^9$

$(0,4)^{10}\ (1,3)^{11}\ (2,2)^{12}\ (3,1)^{13}\ (4,0)^{14}$

$\vdots$

$$(i,j) \leftarrow ? \sum_{x=0}^{i+j} x + i = \frac{(i+j)(i+j+1)}{2} + i$$

$$= \frac{1}{2}[(i+j)^2 + 3i + j]$$

△ The Diagonalization Principle.

The set of real numbers in $(0,1)$ is uncountable. ※

Assume that it is countable.

$r_0 = 0.d_{00}\ d_{01}\ d_{02} \cdots$

$r_1 = 0.d_{10}\ d_{11}\ d_{12} \cdots$

$\vdots$

$r_n = 0.d_{n0}\ d_{n1} \cdots d_{nn} \cdots$

$\vdots$

$S = 0.S_0 S_1 S_2 \cdots \leftarrow S \neq r_i\ \forall i$

$$S_i = \begin{cases} 6 & \text{if } d_{ii} = 7 \\ 7 & \text{otherwise.} \end{cases}$$

A contradiction.

Kim-Man Cha

Power set: The collection of all subsets of a set A.

2^A

$$2^{\{a,b\}} = \{\phi, \{a\}, \{b\}, \{a,b\}\}$$

$2^{\mathbb{N}}$ is uncountable.

$$2^{\mathbb{N}} = \{\phi, \{0\}, \{1\}, \{2\}, \cdots, \{0,2\}, \cdots, \{0,1\}, \{0,2\}, \cdots, \{0,1,2\}, \cdots\}$$

pf. ← Assume that $2^{\mathbb{N}}$ is countable.

$$2^{\mathbb{N}} = \{R_0, R_1, \cdots\}$$

$$D = \{n \in \mathbb{N} : n \notin R_n\}$$

$$D = R_k \Rightarrow \begin{cases} \text{if } k \in R_k \Rightarrow k \notin D \Rightarrow k \notin R_k \\ \text{if } k \notin R_k \Rightarrow k \in D \Rightarrow k \in R_k \end{cases}$$

A contradiction.