CHAPTER 3: METHODS OF PROOF

In this chapter, we shall learn two powerful techniques of proving a result. We shall start with the technique of proof by contradiction, and then move on to the discussion of the Pigeon Hole Principle.

SECTION 3.1. PROOF BY CONTRADICTION.

The basic idea here is to assume ~~that~~ the statement we want to prove is false, and then show that this assumption leads to a nonsense. We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true. It is a special case of a more general form of argument known as Reductio ad Absurdum.

Hardy described proof by contradiction as "one of mathematician's finest weapons." He said that "it is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game".

Let us look at three examples.

Theorem 3.1.1

$\sqrt{2}$ is irrational.

PROOF: Let us suppose, to the contrary, that $\sqrt{2}$ is not irrational i.e. $\sqrt{2}$ is rational. Therefore, there exist $p, q \in \mathbb{N}$ such that

$$\boxed{\sqrt{2} = \frac{p}{q}} \qquad (*)$$

Without loss of generality we may assume that p, q are coprime. Using $(*)$,

$p^2 = 2q^2 \Rightarrow p^2$ is even $\Rightarrow p$ is even. Therefore, for some $k \in \mathbb{N}$, $p = 2k$. Hence, using $(*)$ again,

$4k^2 = p^2 = 2q^2 \Rightarrow q^2$ is even $\Rightarrow q$ is even., which contradicts the fact that p, q are coprime. Hence, $\sqrt{2}$ is irrational. (Proved)

Theorem 3.1.2

Let $a \in \mathbb{R}$, $a \geq 0$ have the property that for all $\epsilon > 0$, $a < \epsilon$. Then, $a = 0$.

PROOF: Let us suppose, to the contrary that $a \neq 0$. i.e. $a > 0$. Let us set $\epsilon := a/2$. Hence, invoking the property of a,

$$0 < a < \frac{a}{2} \quad \text{i.e.}\ 0 < a < 0, \quad \text{a contradiction.}$$

Hence, $a = 0$. (Proved)

Theorem 3.1.3

There are infinitely many primes.

PROOF (EUCLID): Let us suppose, to the contrary, that there are only finitely many prime numbers. Let $p_1 < p_2 < \cdots < p_n$ be the all prime numbers arranged in an increasing order.

Let us define $a \in \mathbb{N}$ by

$$(*) \quad \boxed{a := (p_1 p_2 \cdots p_n) + 1.}$$

Let $a \in \mathbb{N}$ with $a \geq 2$. Hence, a has a prime factor q. Note that, for some $j \in \{1, \ldots, n\}$, $q = p_j$.

We note that q divides $(p_1 p_2 \cdots p_n)$. Since q is a factor of a, q also divides a. Therefore q divides $a - (p_1 p_2 \cdots p_n) = 1$, which is ~~an impossibility~~ absurd.

Therefore, there are infinitely many prime numbers. (Proved)

SECTION 3.2 PIGEON HOLE PRINCIPLE

Let us begin by stating the principle.

Theorem 3.2.1 (PIGEON HOLE PRINCIPLE (PHP))
Let $n, r \in \mathbb{N}$ with $n > r$. If n objects are placed into r boxes, one box will contain more than one objects.

PROOF: Obvious.

The first formalization of PHP is believed to have been made by Dirichlet in 1834 which is why PHP is also known as the Dirichlet Box Principle.

We now look at a few applications of the PHP.

EXAMPLE 3.2.2 (FIVE POINTS ON A UNIT SQUARE)
Given five points on a unit square, there are at least two points at a distance less than or equal to $1/\sqrt{2}$.

PROOF: We divide the square into four subsquares each with side-length $1/2$, and use the PHP.

EXAMPLE 3.2.3 (FOUR POINTS ON A SPHERE)
Given five points on a sphere, at least four points lie on the same hemisphere.

PROOF: Let x_1, x_2, x_3, x_4, x_5 be five points. Consider the two hemispheres determined by the great circle containing x_1, x_2 and 0. Using PHP, at least two x_3, x_4, x_5 lie on one of these two hemispheres determined by the aforementioned great circle. The same hemisphere contains four points.

EXAMPLE 3.2.4
Let $n \in \mathbb{N}$. Any collection of $(n+1)$ integers contains two elements a, b such that n divides $(b-a)$.

Let S be a collection of $(n+1)$ integers. For each $k \in \{0, \dots, n-1\}$, we define.

$$S_k := \{x \in S \mid x \text{ leaves remainder } k \text{ when divided by } n\}.$$

Then, $S = \bigcup_{k=0}^{n-1} S_k$. As S has $(n+1)$ elements, using PHP, there exists $k \in \{0, \dots, n-1\}$ ~~such~~ and $a, b \in S$, ~~such~~ $a \neq b$ ~~that~~ such that $a, b \in S_k$. Then, n divides $(b-a)$.

EXAMPLE 3.2.5

In any group of n people, there are at least two people with the same number of friends.

PROOF: Let S be a group of n people. For each $k \in \{0, \dots, n-1\}$, let us define

$$S_k := \{x \in S \mid x \text{ has exactly } k \text{ friends}\}.$$

Then, $S = \bigcup_{k=0}^{n-1} S_k$. We consider two cases.

CASE 1. $S_0 = \phi$

Then, $S = \bigcup_{k=1}^{n-1} S_k$. Using PHP, there exists $k \in \{1, \dots, n-1\}$ and $x, y \in S$ ~~such~~, $x \neq y$ such that $x, y \in S_k$. Then, x, y both have exactly k number of friends.

CASE 2. $S_0 \neq \phi$

Then, $S_{n-1} = \phi$ i.e. $S = \bigcup_{k=0}^{n-2} S_k$. Using PHP again, we find $k \in \{0, \dots, n-2\}$ and $x, y \in S$, $x \neq y$ such that $x, y \in S_k$. Then, again, x, y both have exactly the same number of friends.

This proves the result. (Proved)

EXAMPLE 3.2.6

Let $n \in \mathbb{N}$ and let $A \subset \{1, 2, \dots, 2n\}$ with exactly $(n+1)$ elements. Then, ~~ex~~ there exist $x, y \in A$ such that x divides y.

PROOF: Let us define, for each $k \in \{1, \dots, n\}$,

$$B_k := \{ 2^j(2k-1) : j \in \mathbb{N}_0 \}.$$

Then, $B_k \cap B_\ell = \phi$, for all $k, \ell \in \{1, \dots, n\}$, $k \neq \ell$ and $A \in \bigcup_{k=1}^{n} B_k$.
Using PHP, there exists $k \in \{1, \dots, n\}$ and $x, y \in A$ with $x \neq y$ such that $x, y \in B_k$. Clearly, either x divides y or y divides x.
This proves the result. (Proved).

5