3. Methods of Proof

"God exists since mathematics is consistent,
and the Devil exists since we cannot prove it."
~ André Weil

In this chapter, we shall learn two powerful techniques which are often useful in proving mathematical results. We shall begin with the technique of proof by contradiction. We shall then discuss the Pigeon Hole Principle.

§3.1. Proof by Contradiction

The basic idea in this method is to assume that the statement we want to prove is false, and then show that this assumption leads to a nonsensical conclusion. We are then forced to conclude that the assumption that "the statement was false" was wrong. It is a special case of a more general form of argument known as Reductio ad Absurdum. The earliest example of a reductio argument can be found in a poem attributed to Xenophanes of Colophon (c. 570 - c. 475 BC)

In Jest

The famous English mathematician G. H. Hardy described proof by contradiction as "one of mathematician's strongest weapons. It is a far finer gambit than any chess manoevre since a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."

Let us look at *four* 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 exists $p, q \in \mathbb{N}$ such that $\sqrt{2} = p/q$. If p & q have common prime factors, we may cancel it and assume that p & q are coprime. Squaring $\sqrt{2} = p/q$ and simplifying, we get

$$p^2 = 2q^2. \qquad \cdots (3\cdot1)$$

Thus, p^2 is an even integer. This implies that 2 divides p^2, whence 2 divides p & p is an even integer. Thus, $p = 2k$ for some integer $k \in \mathbb{N}$. Using eq^n (3·1)

$$4k^2 = 2q^2 \Rightarrow 2k^2 = q^2.$$

This implies q^2 is even, whence q is even. This is a contradiction to p & q being coprime. Thus, $\sqrt{2}$ is irrational. ▨

THEOREM 3·1·2

There are infinitely many primes.

Proof. We shall follow Euclid. Let us suppose, to the contrary, that there exists only finitely many prime numbers, i.e., let $p_1 < p_2 < \cdots < p_k$ be all the prime numbers. Let us define

$$a := (p_1 p_2 \cdots p_k) + 1.$$

As $a \in \mathbb{N}$ and $a \geq 2$, a has a prime factor, say q. Now $q = p_j$ for some $j \in \{1, 2, \ldots, k\}$. Thus,

$$q \mid a \Rightarrow p_j \mid (p_1 \cdots p_k) + 1.$$

This implies p_j divides 1, a contradiction. Therefore, there are infinitely many prime numbers. ▨

THEOREM: There are infinitely many composite numbers.

Proof. Suppose there are finitely many; let $c_1, \ldots, c_k$ be all of them. Consider $c := c_1 \cdots c_k$; this is a new composite number, a contradiction. Careful! Do not, I repeat, do not add 1. ▨

THEOREM 3.1.3

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

Proof. Let us suppose that $a \neq 0$, i.e., $a > 0$. Set $\varepsilon := a/2$ & notice that $0 < a < \varepsilon := a/2$ by the hypothesis on a. But $a < a/2$ is a contradiction. Hence, $a = 0$. ▨

THEOREM 3.1.4

Suppose $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$, then a or b is even.

Proof. Let us suppose, to the contrary, that both a & b are odd. Then a^2 & b^2 are odd and thus c^2, being the sum, is even. As 2 divides c^2, it also divides c. So, 4 divides c^2. But, if $a = 2m+1$ & $b = 2n+1$, then

$$c^2 = a^2 + b^2 = (2m+1)^2 + (2n+1)^2 = 4m^2 + 4m + 1 + 4n^2 + 4n + 1.$$

The right hand side, being c^2, is dividible by 4. As $4m^2 + 4m + 4n^2 + 4n$ is divisible by 4, this forces 2 to be divisible by 4, a contradiction. ▨

§3.2. PIGEON HOLE PRINCIPLE

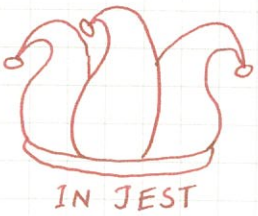
Let us begin by stating the principle.

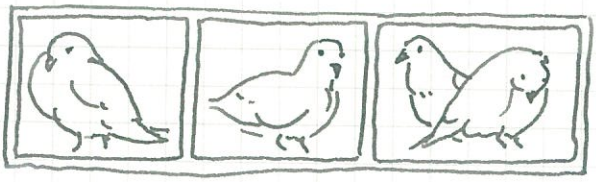
THEOREM 3.2.1 (PIGEON HOLE PRINCIPLE [PHP])

Let $n, r \in \mathbb{N}$ with $n > r$. If n objects are placed into r boxes, at least one box will contain more than one object.

Proof. Let us suppose, to the contrary, that each box contains at most one object. Then the total number of objects is at most r. As $r < n$, the actual number of object, we arrive at a contradiction. ▨

The first formalization of PHP is believed to have been made by Dirichlet in 1834. This is why PHP is often called the Dirichlet box principle.





4 pigeons in
3 pigeon holes

There are several generalizations of PHP. One popular version is as follows: if n objects are placed in m boxes, then at least one box will contain $\lceil n/m \rceil$ many objects, where $\lceil x \rceil$ is the ceiling of x, i.e, the smallest integer greater than or equal to x.

We look at a few applications of PHP.

EXAMPLE 3.2.2

Let $n \in \mathbb{N}$. Any collection of $(n+1)$ integers contains two elements a, b such that n divides $(b-a)$. To prove this, let S be such a set. For each $k \in \{0, 1, \ldots, n-1\}$, define

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

Note that $S = \bigcup_{k=0}^{n-1} S_k$. As S has $(n+1)$ elements, using PHP, there exists $k \in \{0, 1, \ldots, n-1\}$ such S_k has at least two elemen i.e., $a, b \in S_k$. Then n divides $b-a$.

EXAMPLE 3.2.3

Let $n \in \mathbb{N}$ and $A \subset \{1, 2, \ldots, 2n\}$ be a subset with $(n+1)$ elements. Then there exists $x, y \in A$ such that x divides y. To see this, for each $k \in \{1, 2, \ldots, n\}$ define

$$B_k := \{2^j(2k-1) \mid j \in \mathbb{N} \cup \{0\}\}.$$

Note that if $x \in B_k \cap B_\ell$ for $k \neq \ell$ and $k, \ell \in \{1, \ldots, n\}$, then

$$2^{j_1}(2k-1) = x = 2^{j_2}(2\ell-1)$$

If $j_1 = j_2$, then $2k-1 = 2\ell-1$, a contradiction. If $j_1 \neq j_2$, then either $j_1 < j_2$ or $j_2 < j_1$. In the first case, we get

$$2k-1 = 2^{j_2-j_1}(2l-1)$$

which is a contradiction as the left hand side is odd while the right hand side is even. The second case is handled similarly.

As $A \subset \bigcup_{k=1}^{n} B_k$, by PHP, some B_k must contain two elements, say x & y, from A. But then either x divides y or y divides x.

EXAMPLE 3.2.4

In any group of n people, $n \geq 2$ & $n \in \mathbb{N}$, there are at least two people with the same number of friends. To prove this, for each $k \in \{0, \ldots, n-1\}$, define

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

where S is the set of n people. Note that $S = \bigcup_{k=0}^{n-1} S_k$. If $S_{n-1} \neq \emptyset$, then there is a person who is friends with all the rest. Thus, $S_0 = \emptyset$ and using PHP, some S_k has at least two elements, i.e., there exist x & y who have k friends. The only other case is $S_{n-1} = \emptyset$ and using PHP, some S_k for $k \in \{0, 1, \ldots, n-2\}$ has at least two people & we are done.

EXAMPLE 3.2.5

Consider an equilateral triangle of side length 1. Given any five points in it, there will be two points with distance at most $1/2$. To prove this, we divide the triangle into four regions, each an equilateral triangle with side length $1/2$. Note that these overlap along edges &/or vertices.

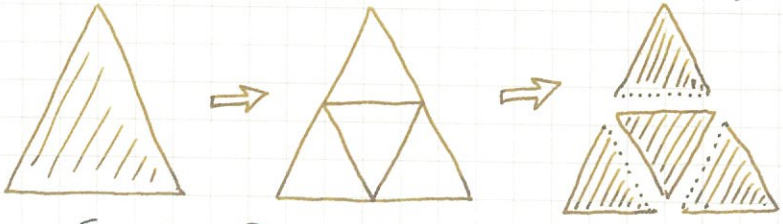


Fig 3.1: Decomposing a triangle into four parts

but we divide it into four disjoint regions, as seen in figure. Using PHP, one of these regions must contain at

least 2 points. But the distance between any two points in an equilateral triangle of side length r is at most r. Thus, there exists two points having distance at most $1/2$.

EXAMPLE 3·2·6 (USA MTS [2006-07] ROUND 1, #4)

Question. Every point in the plane is coloured red, green or blue. Show that there is a rectangle, all of whose vertices have the same colour.

Solution. Consider the grid of points given by

$$S = \{(x,y) \in \mathbb{R}^2 \mid x \in \{0,1,2,3\}, y \in \{0,1,\ldots,81\}\}.$$

Each row in this grid has four points and there are 81 possible ways to colour a row as each point has 3 choices and $81 = 3\times3\times3\times3$. As we have 82 rows, at least two rows must have identical colours. But in each of two rows, one colour must repeat at least twice by PHP. The corresponding vertices form a desired rectangle.